Security Operations

CWL Certified Cyber Security Analyst

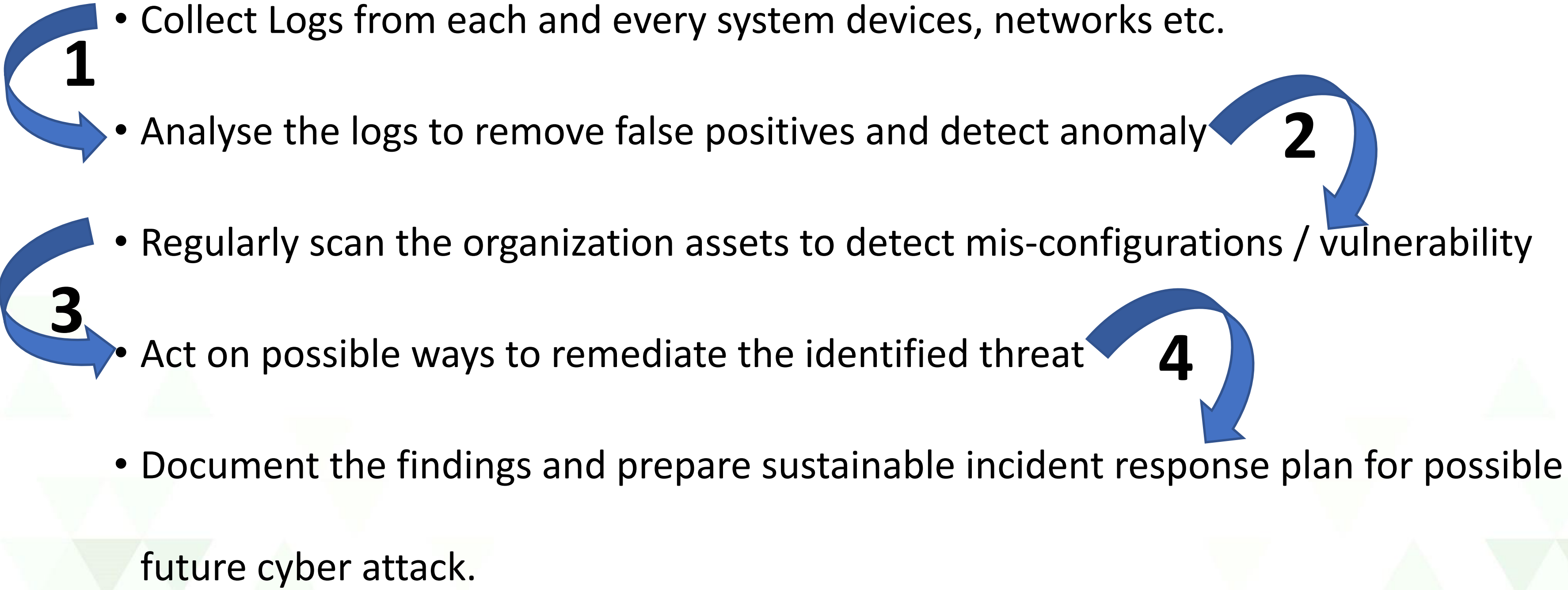
7. Security Operations

Basics of Security Operations

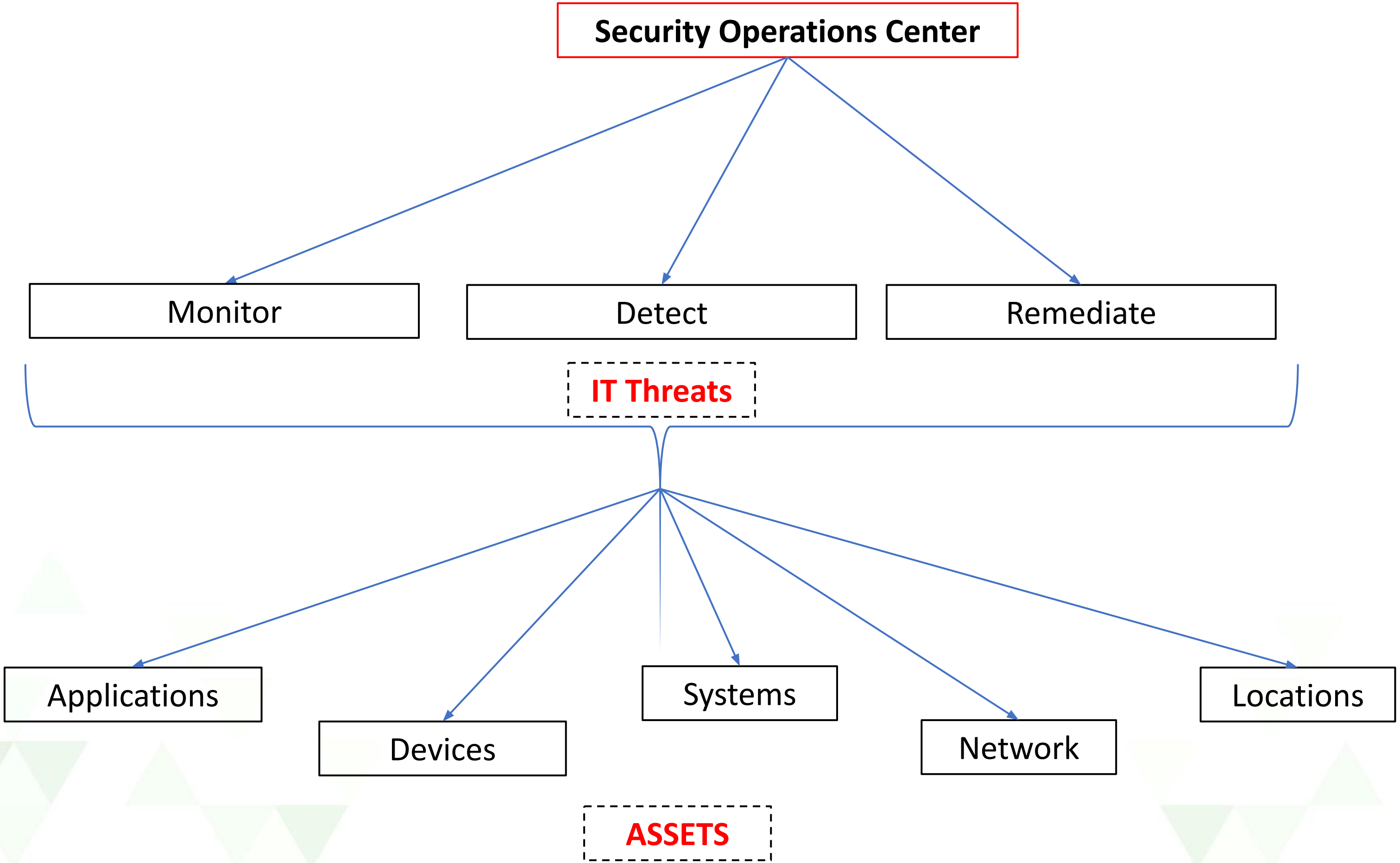
- Security Operations team is responsible for performing defensive activities for the organization
- They aim to protect critical organization assets from threat actors

- Employee equipped with different expertise work together on protecting the organization infrastructure

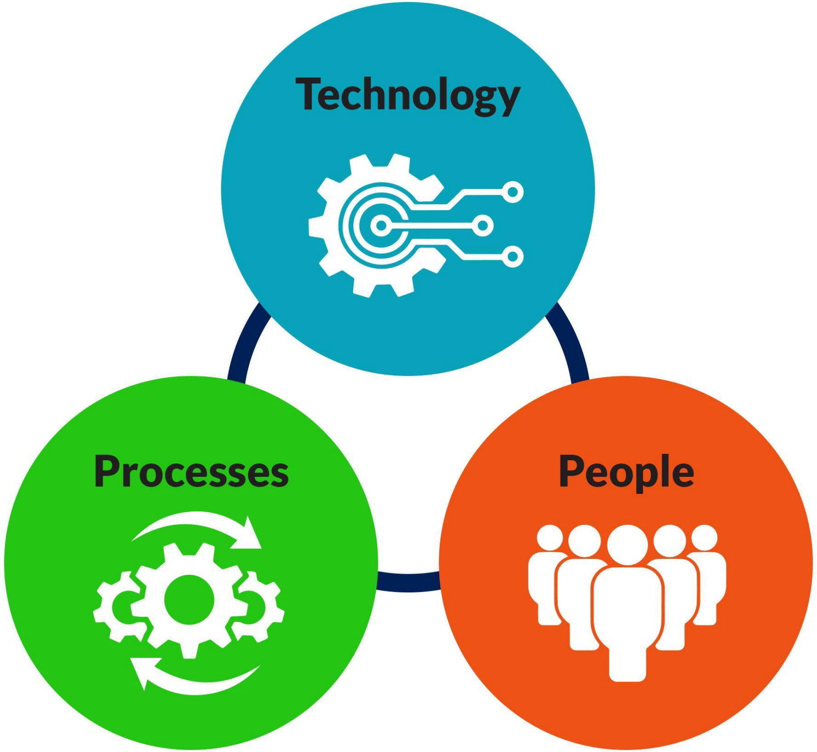
- **SOC procedural workflow :**



  - Collect Logs from each and every system devices, networks etc.
  - Analyse the logs to remove false positives and detect anomaly
  - Regularly scan the organization assets to detect mis-configurations / vulnerability
  - Act on possible ways to remediate the identified threat
  - Document the findings and prepare sustainable incident response plan for possible future cyber attack.


Security Operations Center
Monitor
Detect
Remediate
IT Threats
Applications
Devices
Systems
Network
Locations
ASSETS

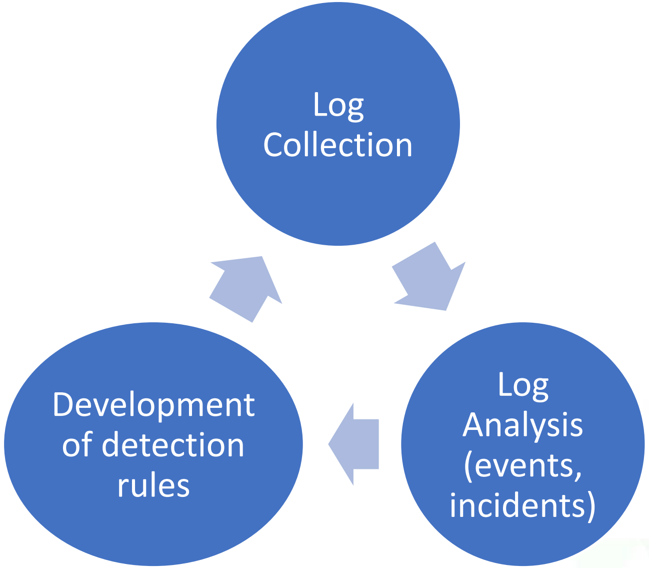
- **<u>Three main functions of SOC</u>**



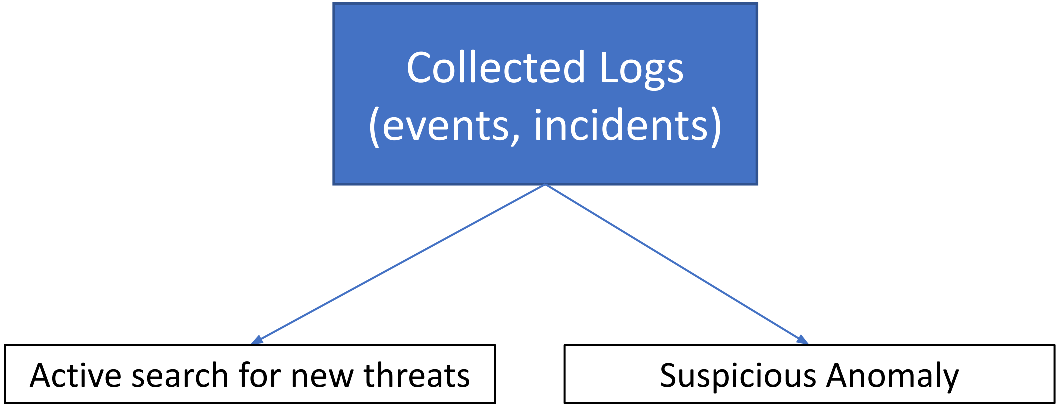
- **Technology**

  - For SOC Team members, technology is their weapon, they use it to collect different type of logs (login events, activities etc).

    - Security Monitoring :


Log Collection
Log Analysis (events, incidents)
Development of detection rules

- **Threat Hunting:**

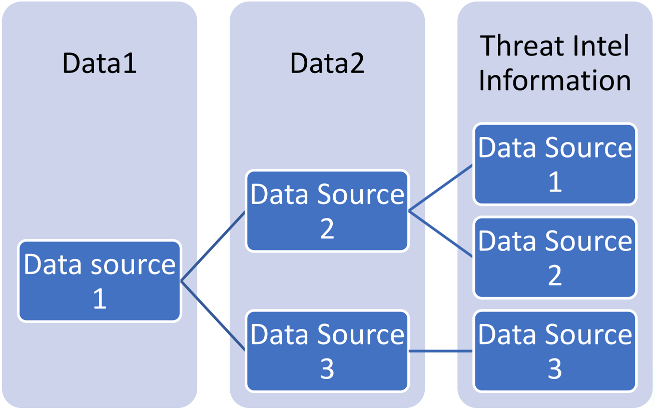


Collected Logs (events, incidents)

Active search for new threats

Suspicious Anomaly

- **Threat Intelligence**



Data1

Data source 1

Data2

Data Source 2

Data Source 3

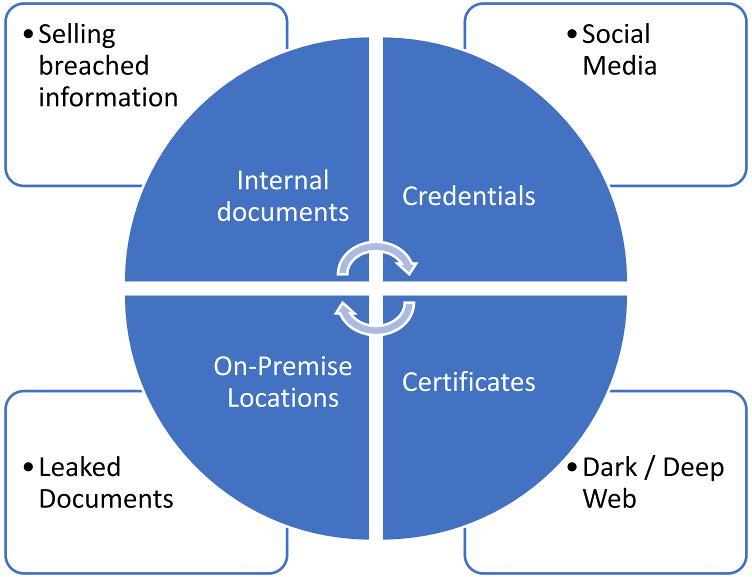
Threat Intel Information

Data Source 1

Data Source 2

Data Source 3

- **Continuous OSINT Gathering**



- Selling breached information

- Social Media

Internal documents

Credentials

On-Premise Locations

Certificates

- Leaked Documents

- Dark / Deep Web

- **People**

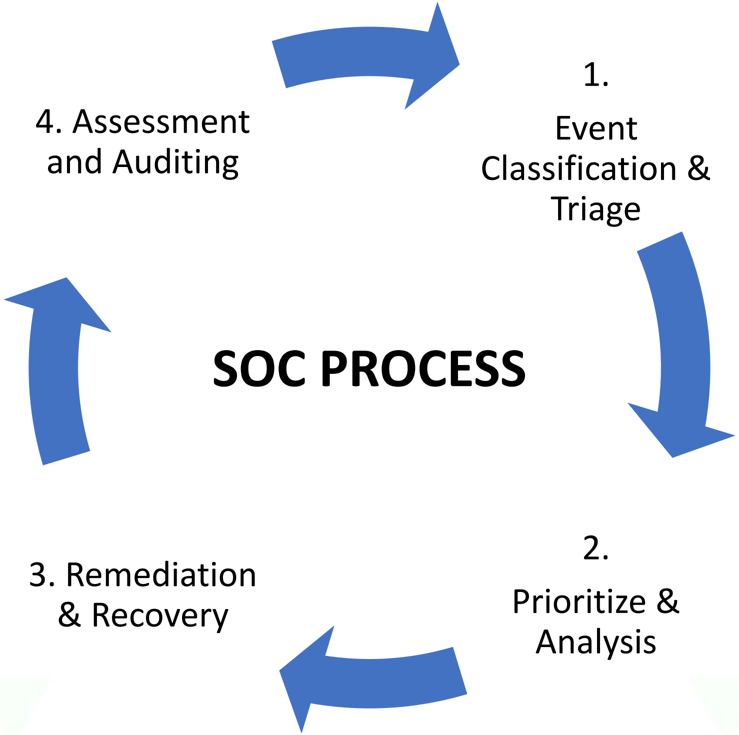
  - Team comprises of people uses least amount of resources to get good visibility into active and emerging threats.

  - Continuous consolidation of technologies and effectively organizing team is required

ROLE	DESCRIPTION	RESPONSIBILITIES
Jr. Security Analyst [Tier-1]	Triaging security incidents	Triage alerts acc. to urgency and relevancy. Manages & configures security monitoring tools
Security Analyst [Tier-2]	Incident Responder	Reviews triaged alerts, identify scope of the alert. Perform remediation and recovery efforts
Senior Security Analyst [Tier-3]	Threat Hunter	Conducts pentesting on production env. Optimizes SOC tools based on threat hunting
SOC Manager	Chief of SOC	Hiring, training & assessing staff. Measures SOC performance & communicates with CISOs

- **Processes**

  - Process ensures timely synchronization and execution of various activities performed by the SOC.



SOC PROCESS

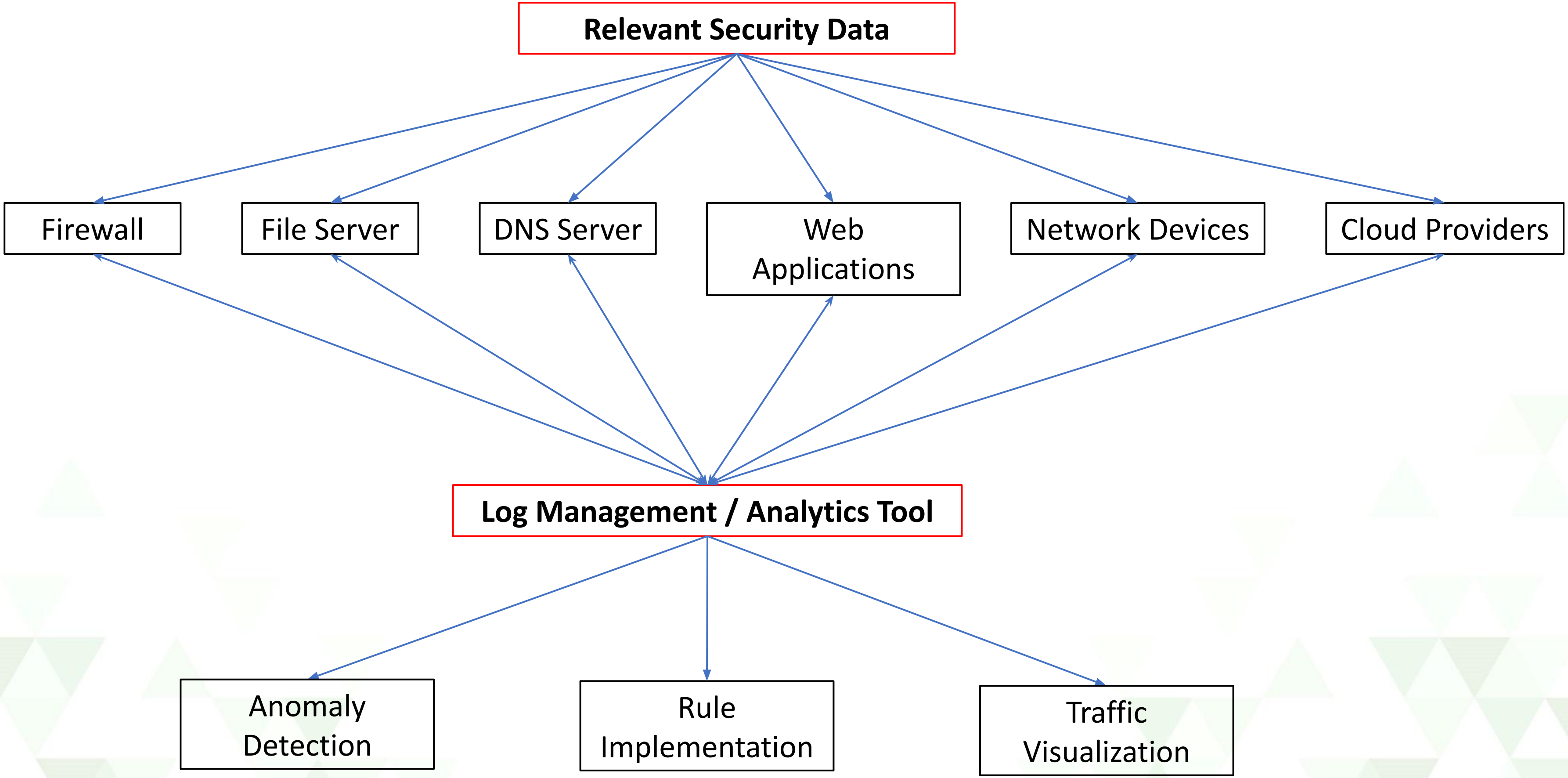
1. Event Classification & Triage

2. Prioritize & Analysis

3. Remediation & Recovery

4. Assessment and Auditing

- **Security Information and Event Management (SIEM) WorkFlow**



- **Industry recognized SIEM Tools**

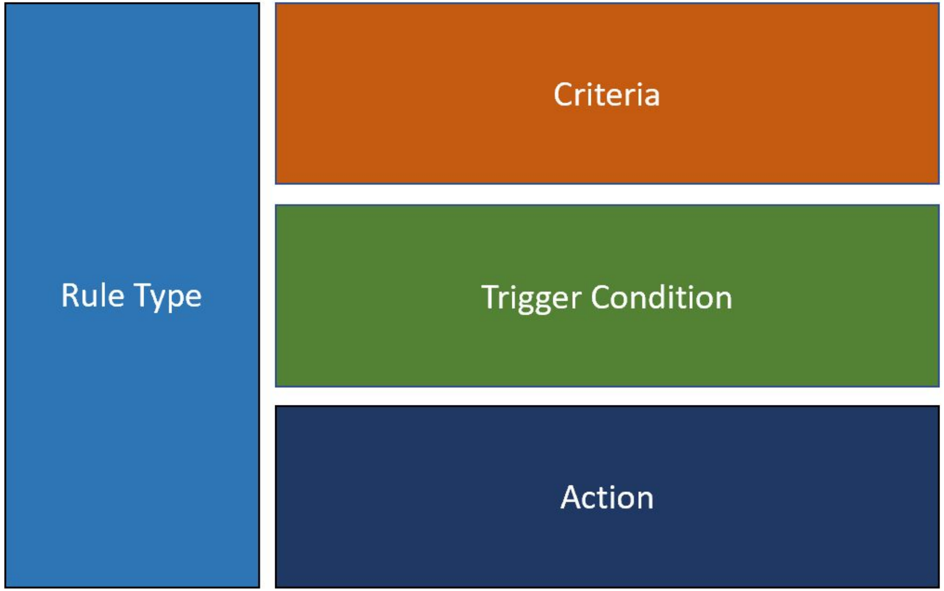
  - Feed data from organization resources and they provide deep level insights of the assets day to day operations

splunk>®

IBM QRadar

MICRO FOCUS ArcSight

- **<u>SIEM Detection Rule</u>**



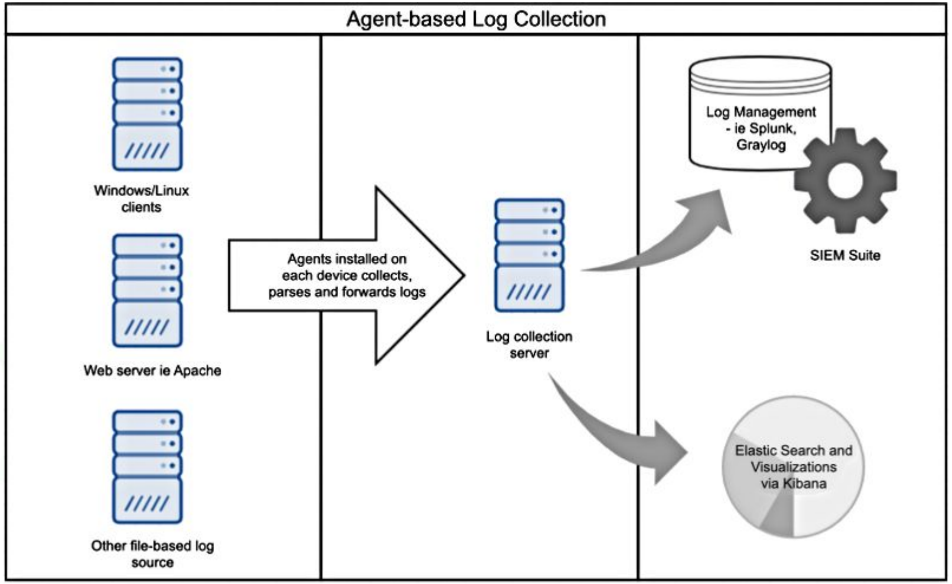
Rule Type

Criteria

Trigger Condition

Action

- **Device integration with SIEM Tools**



Agent-based Log Collection

Windows/Linux clients

Web server ie Apache

Other file-based log source

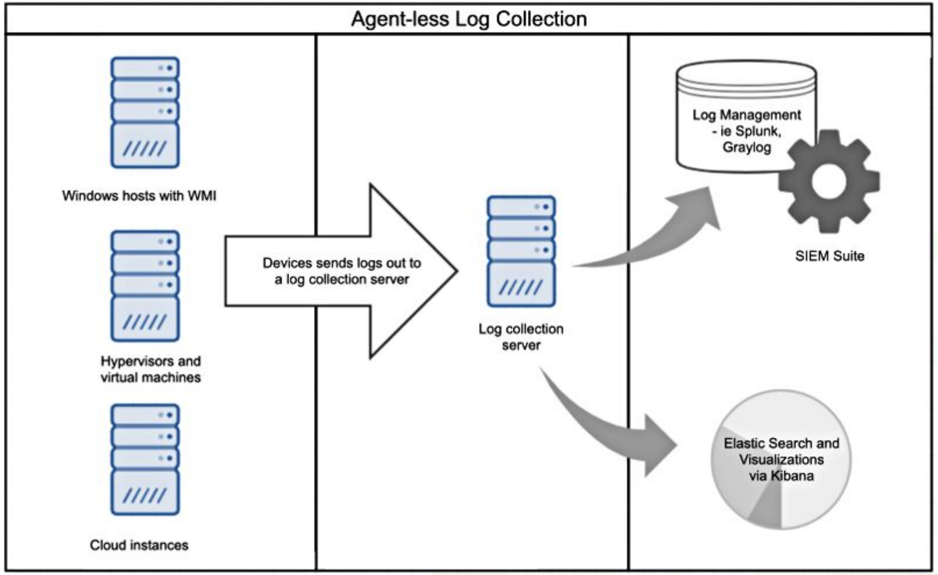
Agents installed on each device collects, parses and forwards logs

Log collection server

Log Management - ie Splunk, Graylog

SIEM Suite

Elastic Search and Visualizations via Kibana



Agent-less Log Collection

Windows hosts with WMI

Hypervisors and virtual machines

Cloud instances

Devices sends logs out to a log collection server

Log collection server

Log Management - ie Splunk, Graylog

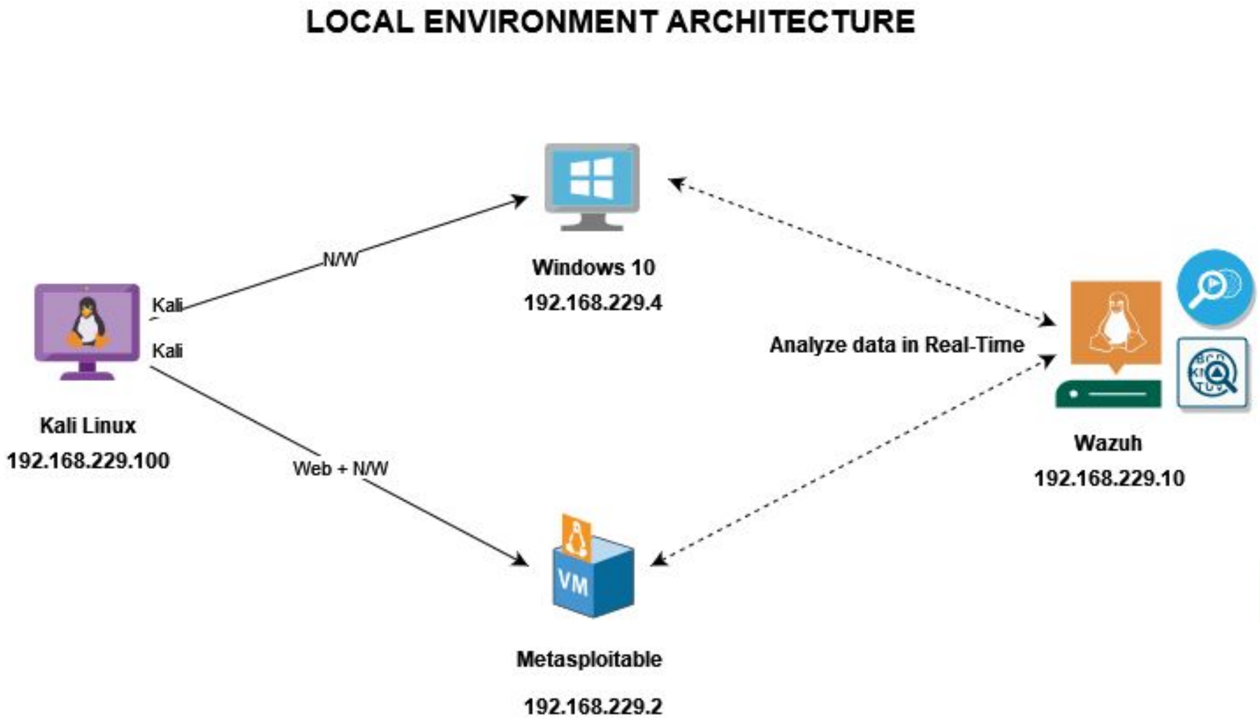
SIEM Suite

Elastic Search and Visualizations via Kibana

Reference : https://nxlog.co/agent-based-versus-agent-less

- **Exercises :**

  - Setting-up the environment for attack and defense visualization



Host based Defence

- Host includes physical / virtual OS that are allocated to the employee of organization
- Enterprise majorly have the following OS’s:
  - Windows
  - Linux
  - Mac
- Tools like OSQuery (cross-platform), Sysmon (Windows) etc can be used to collect and transmit logs for analysing performance of hosts devices.

Host Firewall - Windows

- Defender host firewall present in Win Vista, 7, 8, 10, 11 & server edition.
- It helps secure the devices by in-bound & out-bound rules.
- The rules states which network traffic can go in and out from the device

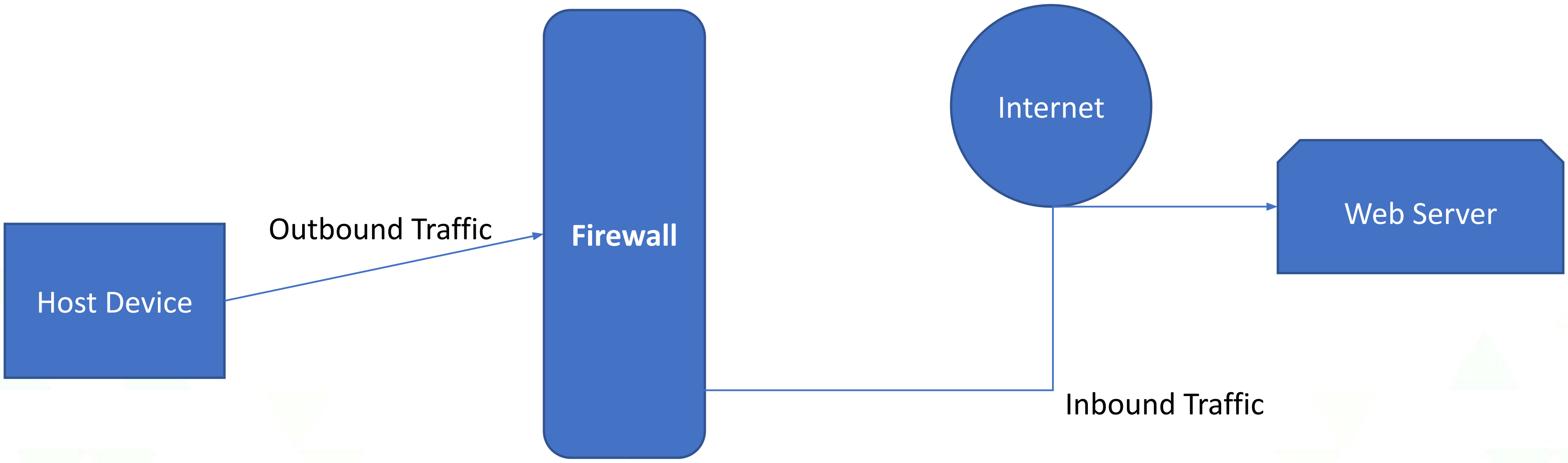
- The firewall works on 3 different network types : Private, Public & Domain

- **Inbound Rules :** Network traffic coming from the external device. Ex : Someone tries to connect to FTP Server on host machine.

- **Outbound rules :** Network traffic originating from the host device. Ex : Host machine tries to connect to a web server.

- **Connection Rules :** Used to filter the network traffic going in and out the host device.

Traffic Flow Diagram



DEMO : Block Google Chrome from accessing the internet

Outbound Setting

Exercise 1 : Isolate Machine from Internet

Inbound Setting

Exercise 2 : Block ICMP packets originating from Internet towards your hosts machine

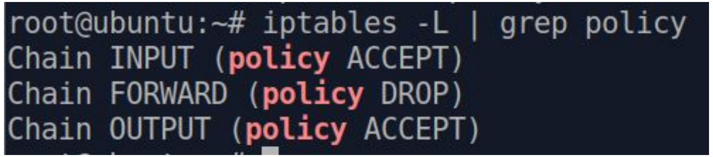
- <u>Host Firewall – iptables</u>

  - Firewall utility that comes in-built in most Linux operating systems.

  - It is a command line utility, that filters network traffic going-in or going-out of the system.

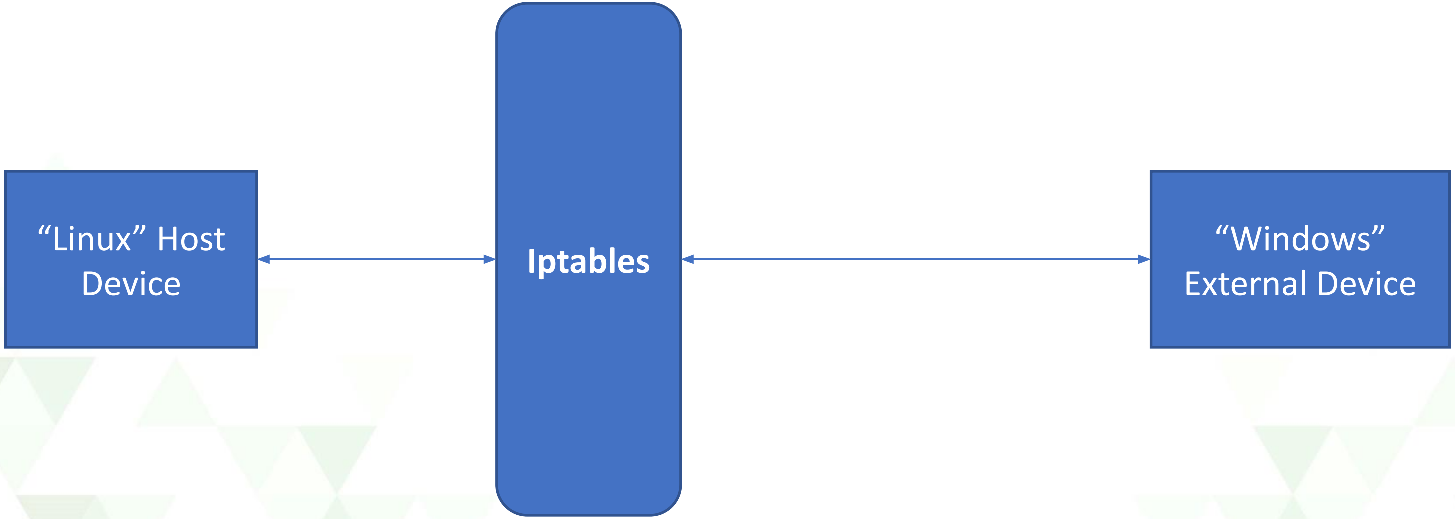
  - Iptables has 3 different chains, namely:
    - Input : Controls incoming connections. Ex : SSH into host machine with iptables enabled
    - Output : Controls outgoing connections. Ex : Sending ICMP packets to a destination
    - Forward : Helpful during routing scenarios, utilizes traffic forwarding utilities to sent data to destined address.

- Check the current configuration of iptables.

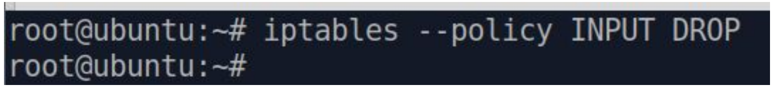


```
root@ubuntu:~# iptables -L | grep policy
Chain INPUT (policy ACCEPT)
Chain FORWARD (policy DROP)
Chain OUTPUT (policy ACCEPT)
```

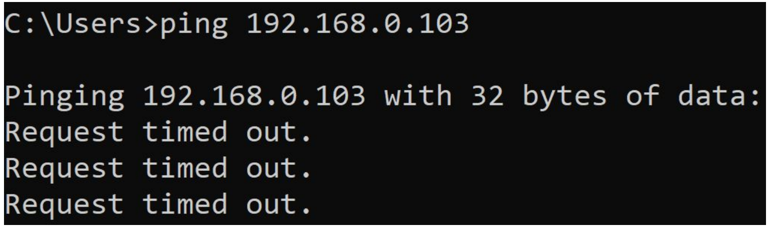
- Iptable accept, deny chains:



- **DROP** the connection in **INPUT** chain :

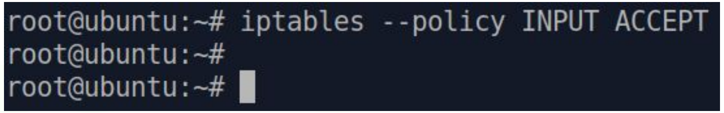


```
root@ubuntu:~# iptables --policy INPUT DROP
root@ubuntu:~#
```

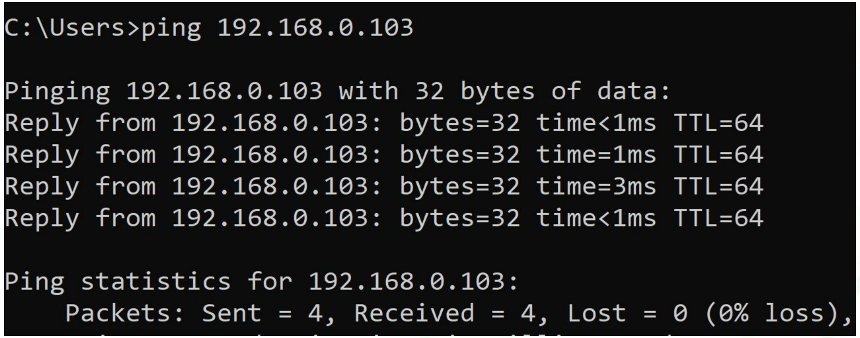


```
C:\Users>ping 192.168.0.103

Pinging 192.168.0.103 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
```

- **ACCEPT** the connection in **INPUT** chain :

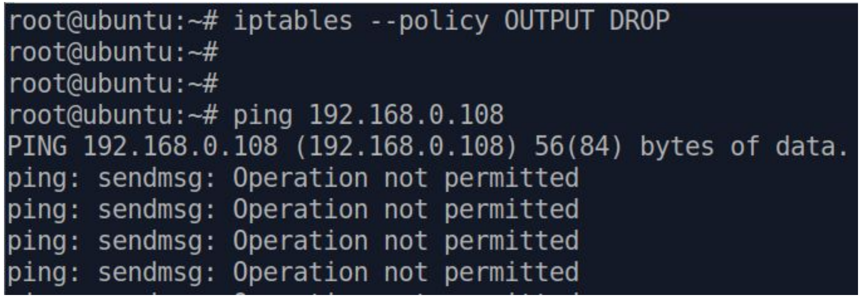


```
root@ubuntu:~# iptables --policy INPUT ACCEPT
root@ubuntu:~#
root@ubuntu:~# 
```



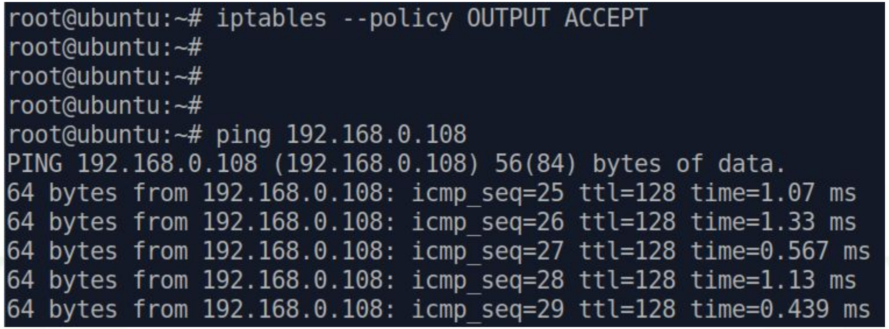
```
C:\Users>ping 192.168.0.103

Pinging 192.168.0.103 with 32 bytes of data:
Reply from 192.168.0.103: bytes=32 time<1ms TTL=64
Reply from 192.168.0.103: bytes=32 time=1ms TTL=64
Reply from 192.168.0.103: bytes=32 time=3ms TTL=64
Reply from 192.168.0.103: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.103:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

- **DROP** the connection in **OUTPUT** chain :



```
root@ubuntu:~# iptables --policy OUTPUT DROP
root@ubuntu:~#
root@ubuntu:~#
root@ubuntu:~# ping 192.168.0.108
PING 192.168.0.108 (192.168.0.108) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
```

- **ACCEPT** the connection in **INPUT** chain :

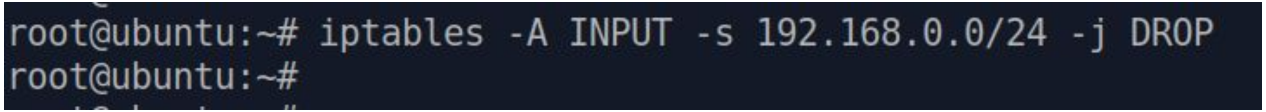


```
root@ubuntu:~# iptables --policy OUTPUT ACCEPT
root@ubuntu:~#
root@ubuntu:~#
root@ubuntu:~#
root@ubuntu:~# ping 192.168.0.108
PING 192.168.0.108 (192.168.0.108) 56(84) bytes of data.
64 bytes from 192.168.0.108: icmp_seq=25 ttl=128 time=1.07 ms
64 bytes from 192.168.0.108: icmp_seq=26 ttl=128 time=1.33 ms
64 bytes from 192.168.0.108: icmp_seq=27 ttl=128 time=0.567 ms
64 bytes from 192.168.0.108: icmp_seq=28 ttl=128 time=1.13 ms
64 bytes from 192.168.0.108: icmp_seq=29 ttl=128 time=0.439 ms
```

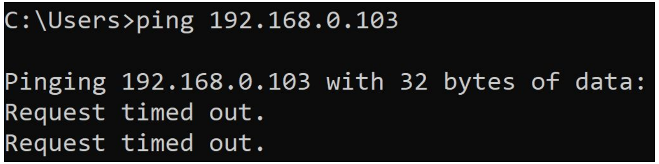
- Connection Specific Responses

  - **ACCEPT** : Allow the connection
  - **DROP** : Drop the connection without sending any errors
  - **REJECT** : Drop the connection but send back an error response

- Block connection from a range of IP address:

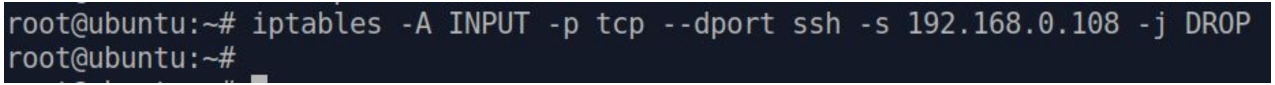


```
root@ubuntu:~# iptables -A INPUT -s 192.168.0.0/24 -j DROP
root@ubuntu:~#
```

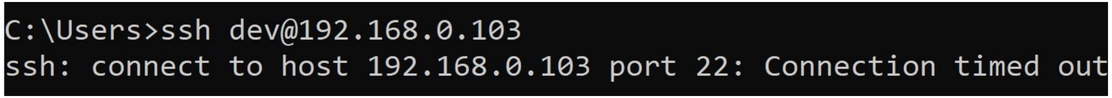


```
C:\Users>ping 192.168.0.103

Pinging 192.168.0.103 with 32 bytes of data:
Request timed out.
Request timed out.
```

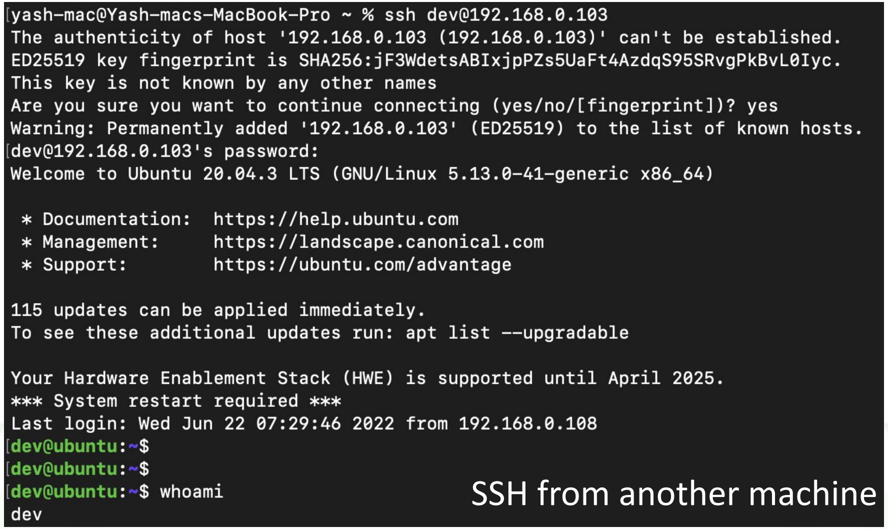
- Block connection to a specific service port (SSH) over TCP



```
root@ubuntu:~# iptables -A INPUT -p tcp --dport ssh -s 192.168.0.108 -j DROP
root@ubuntu:~#
```



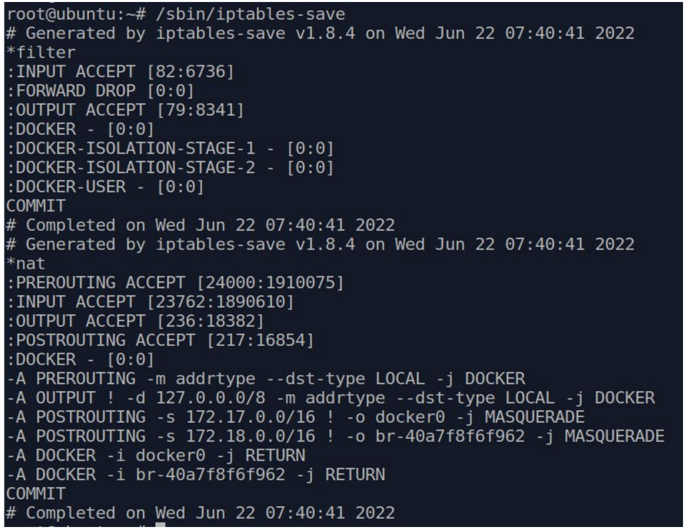
```
C:\Users>ssh dev@192.168.0.103
ssh: connect to host 192.168.0.103 port 22: Connection timed out
```



```
[yash-mac@Yash-macs-MacBook-Pro ~ % ssh dev@192.168.0.103
The authenticity of host '192.168.0.103 (192.168.0.103)' can't be established.
ED25519 key fingerprint is SHA256:jF3WdetsABIxjpPZs5UaFt4AzdqS95SRvgPkBvL0Iyc.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.103' (ED25519) to the list of known hosts.
[dev@192.168.0.103's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.13.0-41-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

115 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.
*** System restart required ***
Last login: Wed Jun 22 07:29:46 2022 from 192.168.0.108
[dev@ubuntu:~$
[dev@ubuntu:~$
[dev@ubuntu:~$ whoami
dev
```

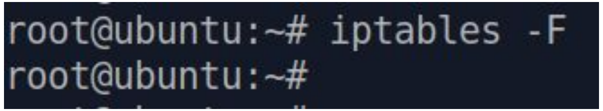
SSH from another machine

- Save the configured rules



```
root@ubuntu:~# /sbin/iptables-save
# Generated by iptables-save v1.8.4 on Wed Jun 22 07:40:41 2022
*filter
:INPUT ACCEPT [82:6736]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [79:8341]
:DOCKER - [0:0]
:DOCKER-ISOLATION-STAGE-1 - [0:0]
:DOCKER-ISOLATION-STAGE-2 - [0:0]
:DOCKER-USER - [0:0]
COMMIT
# Completed on Wed Jun 22 07:40:41 2022
# Generated by iptables-save v1.8.4 on Wed Jun 22 07:40:41 2022
*nat
:PREROUTING ACCEPT [24000:1910075]
:INPUT ACCEPT [23762:1890610]
:OUTPUT ACCEPT [236:18382]
:POSTROUTING ACCEPT [217:16854]
:DOCKER - [0:0]
-A PREROUTING -m addrtype --dst-type LOCAL -j DOCKER
-A OUTPUT ! -d 127.0.0.0/8 -m addrtype --dst-type LOCAL -j DOCKER
-A POSTROUTING -s 172.17.0.0/16 ! -o docker0 -j MASQUERADE
-A POSTROUTING -s 172.18.0.0/16 ! -o br-40a7f8f6f962 -j MASQUERADE
-A DOCKER -i docker0 -j RETURN
-A DOCKER -i br-40a7f8f6f962 -j RETURN
COMMIT
# Completed on Wed Jun 22 07:40:41 2022
```

- Flush the rules:



```
root@ubuntu:~# iptables -F
root@ubuntu:~#
```

OUTPUT Setting

Exercise 1 : Block ICMP packets using iptables

INPUT Setting

Exercise 2 : Block ICMP packets originating from Internet towards your hosts machine

- **Anti-Virus**

  - In General Terms, it is a computer program used to prevent, detect and remove malicious s/w.
  - They continuously scan incoming files (coming to system from everywhere) and if any anomaly is detected, it is quarantined / removed.
  - The Landscape of security has moved a lot from focusing only a single device to end-point devices like Cell-phone, Enterprise laptop, Tablet, Servers, Computers etc.
  - End Point Security protects network, using a combination of FireWall, AntiVirus, Anti-Malware etc.
  - They are explicitly designed for enterprise clients to protect all their endpoints devices like servers, computers, mobile etc.

Endpoint Detection & Response (EDR)

- Understanding Naming Context, it is clear that **EDR** is a solution that continuously monitors, stores endpoint-devices behaviour to detect and block suspicious / malicious activities and also provides remediation facilities all at one place (single dashboard).

- Some unique key features of EDR are :
  - **Visibility**
  - **Continuously updating Telemetry Database**
  - **EDR Focus more on Indicator of Attack (IOA, Detecting the intention of an Adversary)**
  - **Detailed Insights to the environment**
  - **Precision & Accuracy in response**
  - **Integrated with Cloud Based Solution**
  - **Real-Time Monitoring and insights on a single dashboard**

Visibility
Real-Time Monitoring and insights on a single dashboard
Detailed Insights to the environment
Integrated with Cloud Based Solution
Precision & Accuracy in response
Continuously updating Telemetry Database
EDR Focus more on Indicator of Attack
(IOA, Detecting the intention of an Adversary)

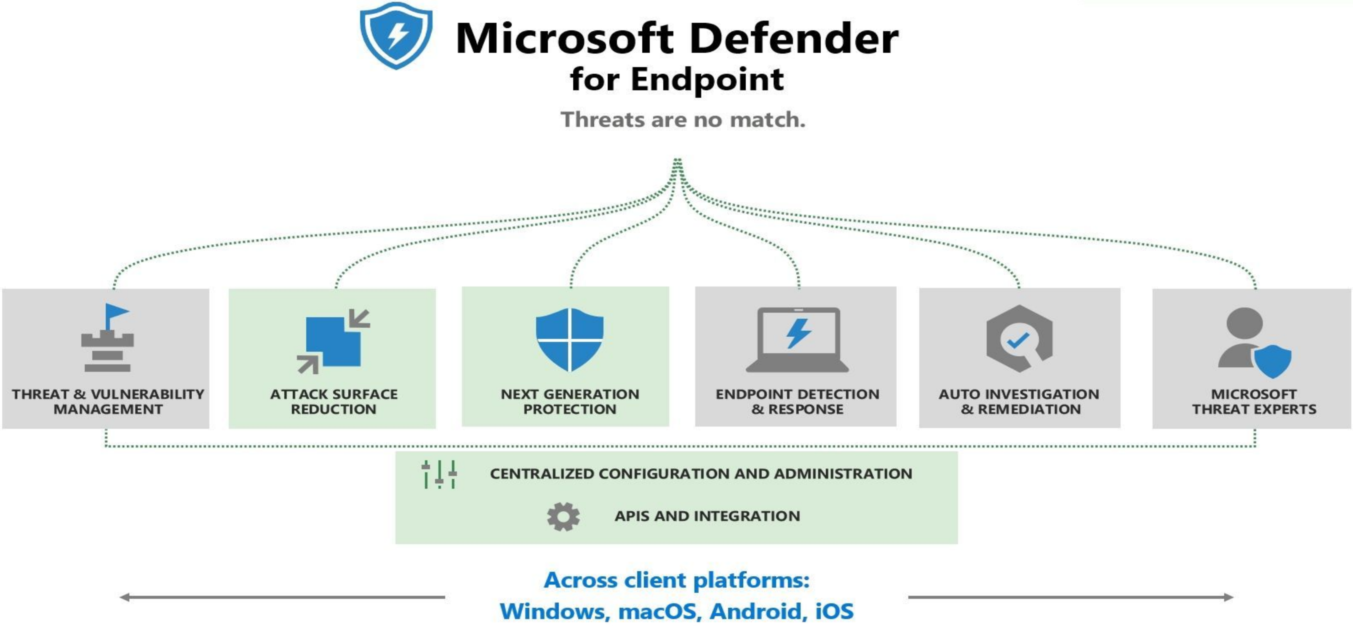
- But why?
  - **Big enterprises with more endpoint devices have more sensitive data**
  - **Adversaries targeting endpoint servers / computers to establish foothold**
  - **Detailed Insights to the environment**
  - **Enterprise Adoption of SaaS based solutions is growing**
  - **More Scalability and ease of configuration**
  - **EDR includes fine-tuned multiple security solutions (focus on consolidation)**

- Examples of EDR in market (not particularly in order of performance):
  - **FireEye Endpoint Security**
  - **CrowdStrike Falcon Insight**
  - **Microsoft Defender Advanced Threat Protection (ATP)**
  - **VMware Carbon Black EDR**
  - **Symantec Endpoint Protection**
  - **SolarWinds Endpoint Detection and Response etc**

Microsoft Defender for Endpoint

- Centralized platform to manage all the organization endpoint devices in a single dashboard
- Works on agent based methodology, it needs to be installed on endpoints which collects the data & send the telemetry to dashboard

Plan 1 capabilities

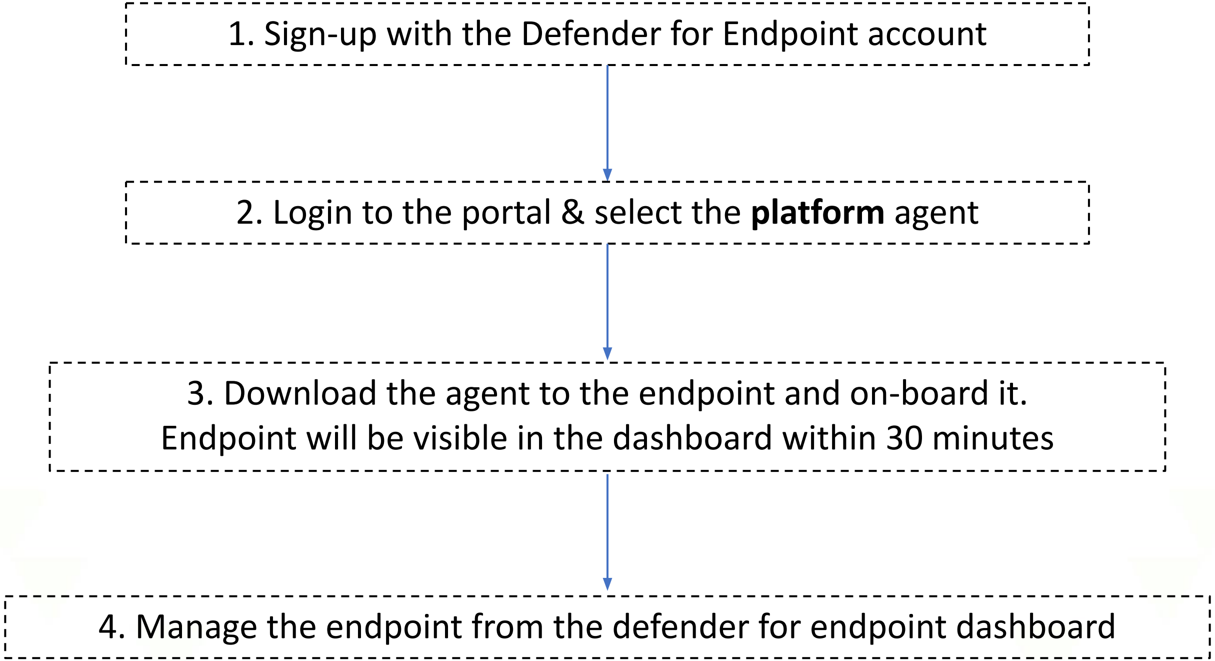


Microsoft Defender for Endpoint

Threats are no match.

THREAT & VULNERABILITY MANAGEMENT
ATTACK SURFACE REDUCTION
NEXT GENERATION PROTECTION
ENDPOINT DETECTION & RESPONSE
AUTO INVESTIGATION & REMEDIATION
MICROSOFT THREAT EXPERTS
CENTRALIZED CONFIGURATION AND ADMINISTRATION
APIS AND INTEGRATION
Across client platforms:
Windows, macOS, Android, iOS

Microsoft Defender for Endpoint sign-up procedure



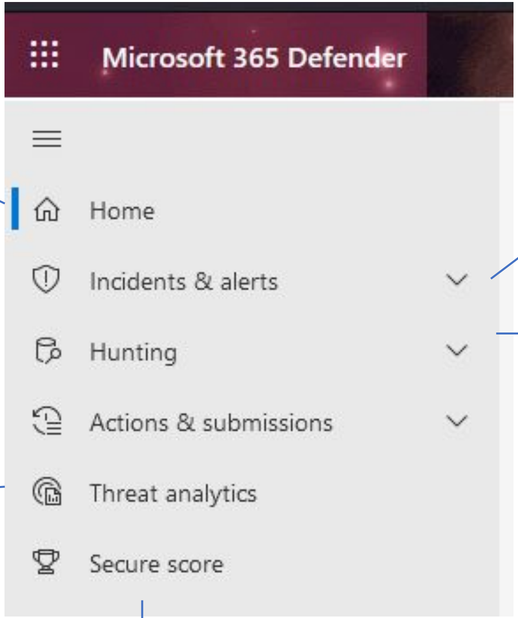
1. Sign-up with the Defender for Endpoint account

2. Login to the portal & select the **platform** agent

3. Download the agent to the endpoint and on-board it.
Endpoint will be visible in the dashboard within 30 minutes

4. Manage the endpoint from the defender for endpoint dashboard

Defender Dashboard



Prioritize Alerts & Check incidents

Write custom queries to track missed alerts

Overall threat Analytics of on boarded endpoints

Score as per MS recommendations

DEMO : MS Defender for Endpoint Demonstration

Exercise 1

Onboard a Windows Machine and check it’s status in dashboard

Exercise 2

Onboard a Linux Machine and check it’s status in dashboard

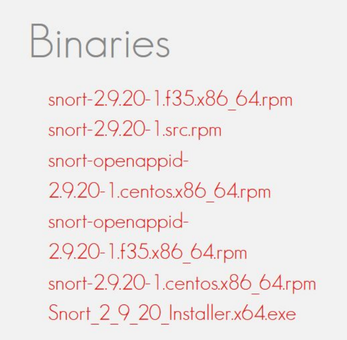
Network based Defence

- Network comprises of multiple hosts present in the organization
- Network are segregated using firewalls, switches etc
- Collecting logs from network devices becomes difficult as they have a ton of data regularly processing in the production

- Snort

  - Open-Source Intrusion prevention system (IPS) developed by Cisco
  - This software is capable of performing real-time traffic analysis and packet logging on IP networks
  - It can also be used to detect a variety of attacks and probes
  - It has 3 modes:
    - Packet Sniffer (like tcpdump)
    - Packet Logger
    - Full-blown IPS

- Download the software from here: https://www.snort.org/downloads



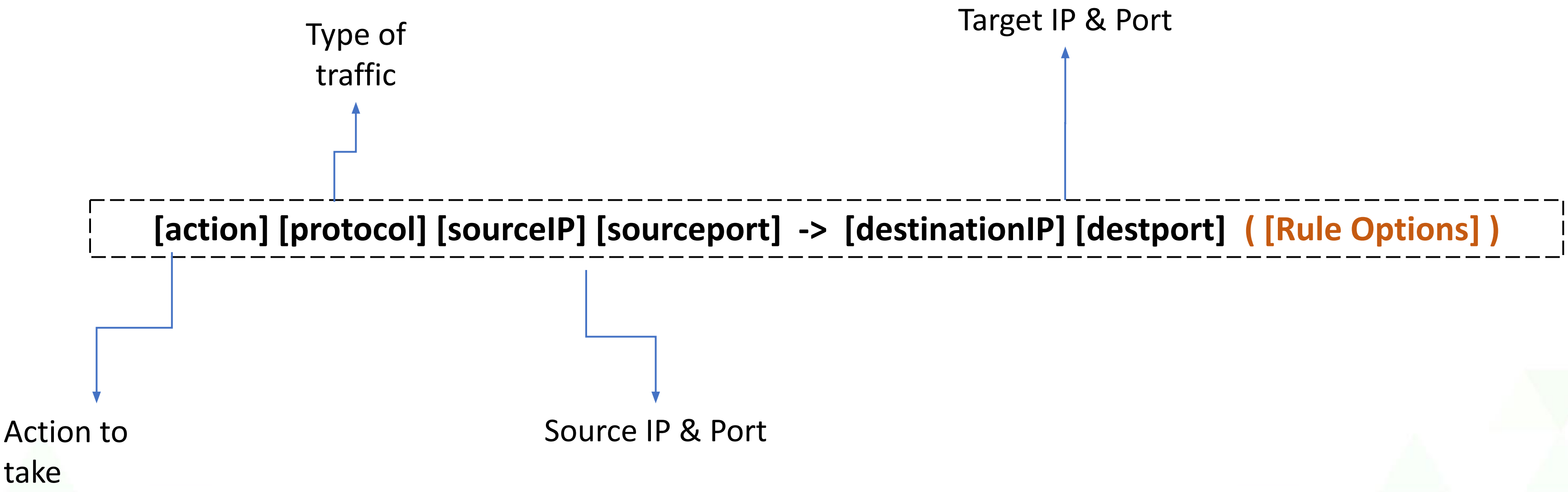
Binaries

snort-2.9.20-1.f35.x86_64.rpm
snort-2.9.20-1.src.rpm
snort-openappid-2.9.20-1.centos.x86_64.rpm
snort-openappid-2.9.20-1.f35.x86_64.rpm
snort-2.9.20-1.centos.x86_64.rpm
Snort_2_9_20_Installer.x64.exe

- The software can also be downloaded using the apt from already added repository

- Snort performs real-time monitoring of packets using rules that are present in the configuration file.

Snort Rule Header



[action] [protocol] [sourceIP] [sourceport] -> [destinationIP] [destport] ([Rule Options])

Snort Rule Header Example

```
alert tcp $sourceIP $sourceport  ->  $destinationIP any
```

Snort Rule Options

General Rule Options

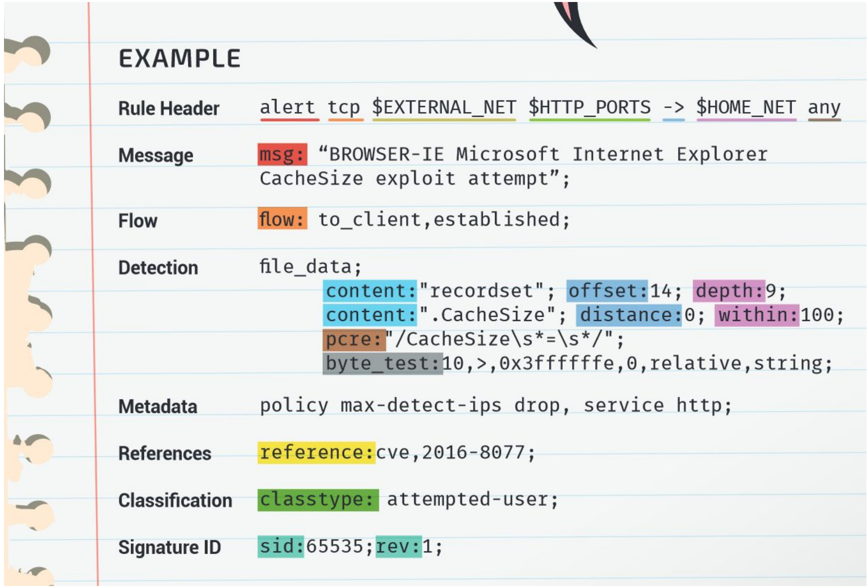
Message: Meaningful **msg** stating the purpose of rule

sid / rev: Unique identified for each rule

Classtype : What the effect of successful attack would be

Reference : External source of information

Reference : For the rule to fire, specifies which direction the network traffic is going.



EXAMPLE

Rule Header	alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any
Message	msg: “BROWSER-IE Microsoft Internet Explorer CacheSize exploit attempt”;
Flow	flow: to_client,established;

Detection	file_data;
	content:"recordset"; offset:14; depth:9;
	content:".CacheSize"; distance:0; within:100;
	pcre:"/CacheSize\s*=\s*/";
	byte_test:10,>,0x3ffffffe,0,relative,string;

Metadata	policy max-detect-ips drop, service http;
References	reference:cve,2016-8077;
Classification	classtype: attempted-user;
Signature ID	sid:65535;rev:1;

[Snort Infographic]

Detection Rule Options

Content: Search for a specific content in the packet payload

pcre : Regular expresssions

Byte Test : It allows a rule to test a number of bytes against a specific value in binar

- Snort configuration file location

/etc/snort/snort.conf

- Edit custom snort rules

/etc/snort/rules/local.rules

- Adding a rule in the **local.rules**

```
alert icmp any any -> 192.168.1.8 any (msg:”ICMP Test”; sid: 1000001; rev:1;)
```

- Starting snort and capturing traffic as per configured rules

```
sudo snort –T –i eth0 –c /etc/snort/snort.conf
```

```
sudo snort –A console –q –i eth0 –c /etc/snort/snort.conf
```

DEMO : Detect SSH Login Attempt

Exercise 1

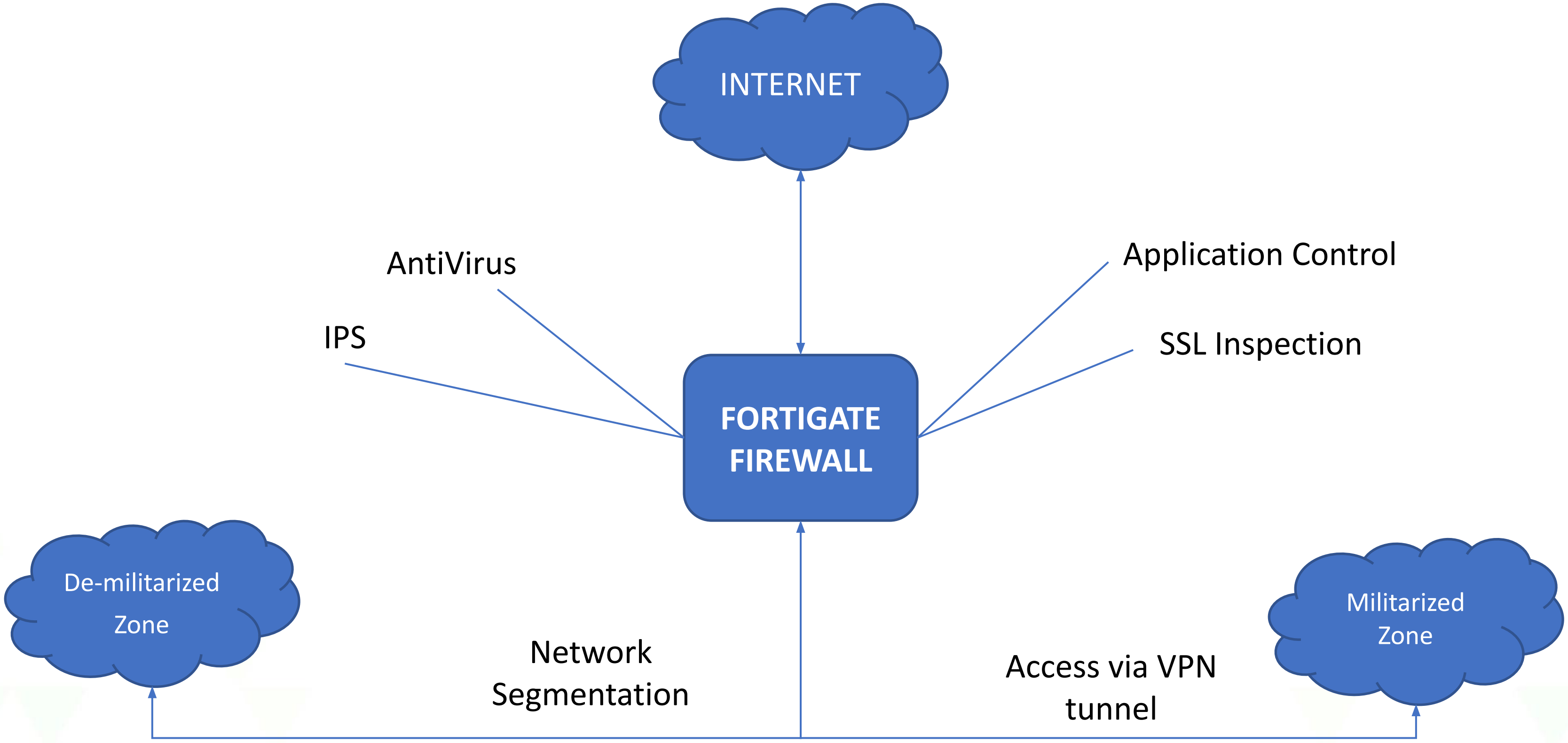
Detect ICMP packet heading towards the snort installed machine

https://www.youtube.com/watch?v=8lOTUqfkAhQ

Exercise 2

Detect failed FTP attempt using alert type

- Fortinet Fortigate Firewall
  - Next-Generation firewall that provides ultimate threat protection for businesses
  - Mainly used in enterprises for the following purposes:
    - VPN tunnels
    - Network segmentation
    - **Web Filtering**
    - Secure Firewall Portal Access
    - Easy integration with other Fortinet products


INTERNET
AntiVirus
Application Control
IPS
SSL Inspection
FORTIGATE FIREWALL
De-militarized Zone
Militarized Zone
Network Segmentation
Access via VPN tunnel

Exercise 1

Fortinet Fortigate Dashboard Demonstration

Exercise 2

Fortinet Fortigate Abuse Demonstration (RCE)

- Security Information and Event Management – Splunk

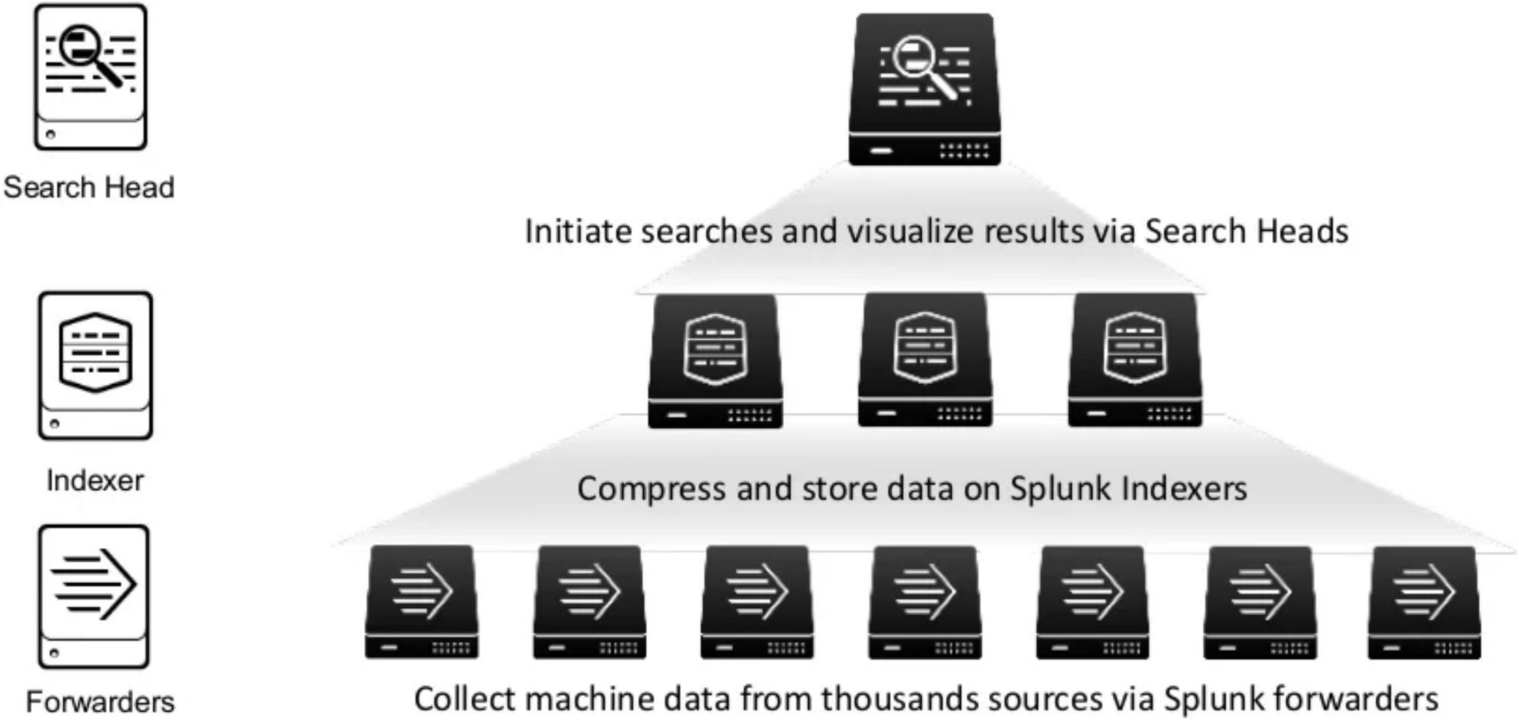
  - It provides real-time data to perform analysis based on security events

  - Tools like Splunk matches collected events against rules & analytics engines to detect & analyse advanced threats

  - Alert indexing is an important aspect that is covered by Splunk. It integrates the events into alert workflow procedure

  - Splunk and SIEM can be deployed in
    - Single environment
    - Distributed environment

- <u>Splunk Working Modes</u>



Search Head

Indexer

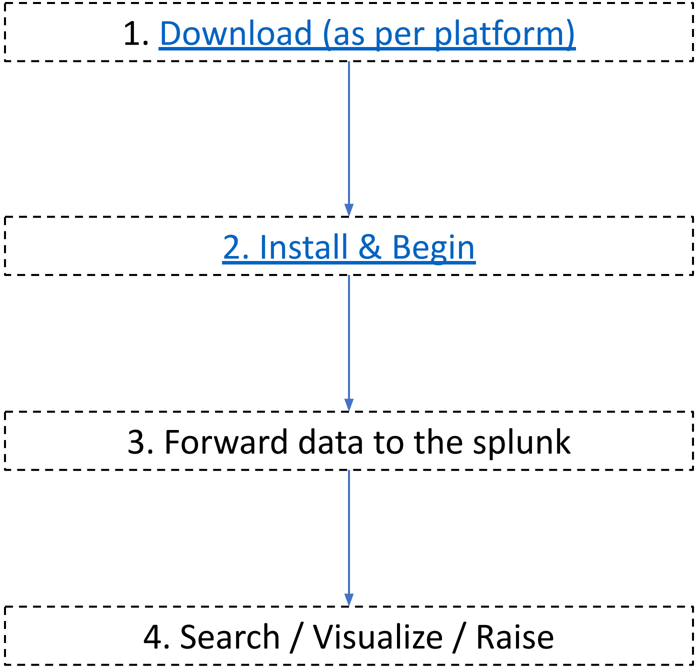
Forwarders

Initiate searches and visualize results via Search Heads

Compress and store data on Splunk Indexers

Collect machine data from thousands sources via Splunk forwarders

- Configuring Splunk

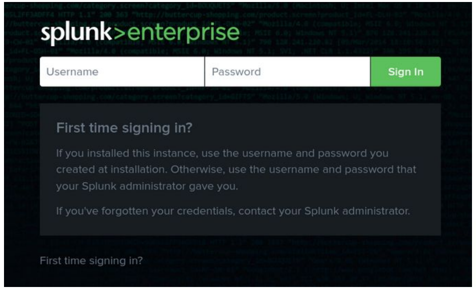


1. Download (as per platform)

2. Install & Begin

3. Forward data to the splunk

4. Search / Visualize / Raise



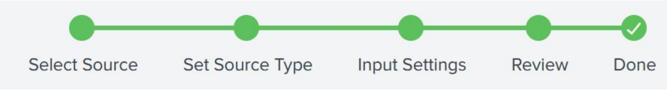
First time signing in?

If you installed this instance, use the username and password you created at installation. Otherwise, use the username and password that your Splunk administrator gave you.

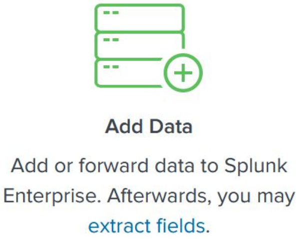
If you've forgotten your credentials, contact your Splunk administrator.

First time signing in?

Log Collection in Splunk (local setup)



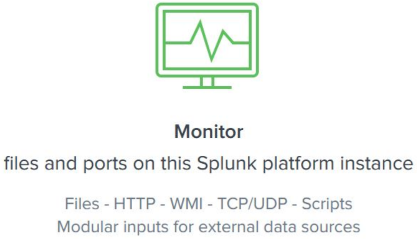
- Select the following icon after signing up



Add Data

Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

- Navigate and choose the “**Monitor**” option, it will monitor the local splunk platform instance

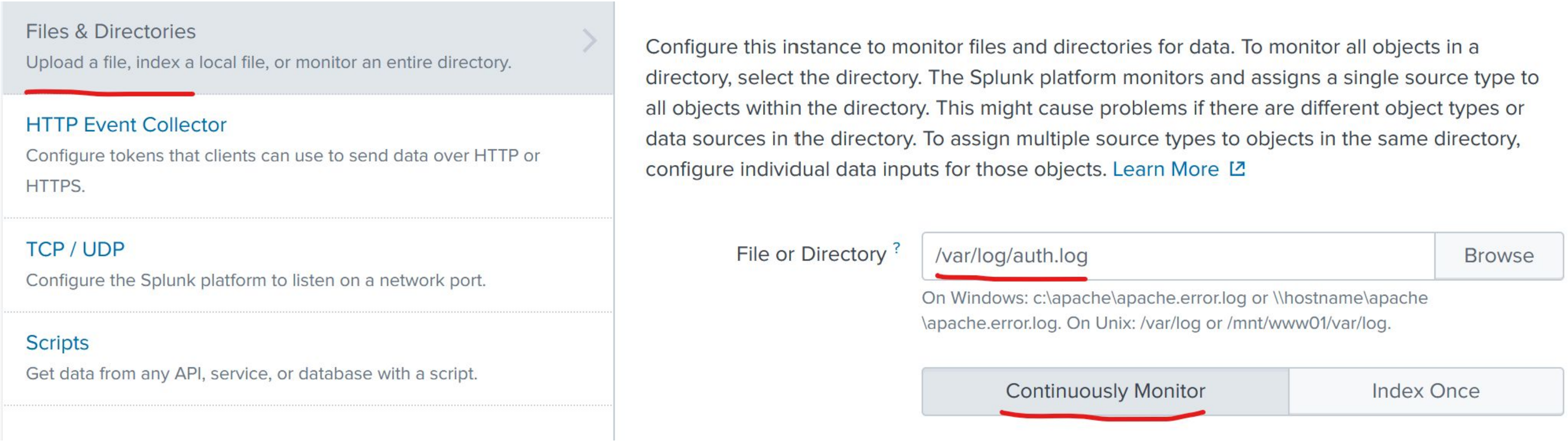


Monitor

files and ports on this Splunk platform instance

Files - HTTP - WMI - TCP/UDP - Scripts
Modular inputs for external data sources

- Choose the auth.log file that collects login attempts locally



Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure the Splunk platform to listen on a network port.

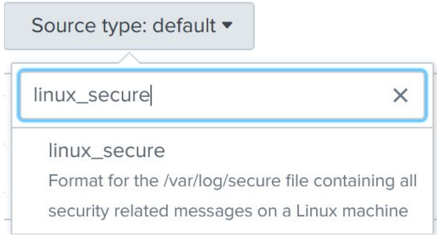
Scripts
Get data from any API, service, or database with a script.

Configure this instance to monitor files and directories for data. To monitor all objects in a directory, select the directory. The Splunk platform monitors and assigns a single source type to all objects within the directory. This might cause problems if there are different object types or data sources in the directory. To assign multiple source types to objects in the same directory, configure individual data inputs for those objects. Learn More

File or Directory ?: /var/log/auth.log

On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.

- Select the source type as “**linux_secure**”

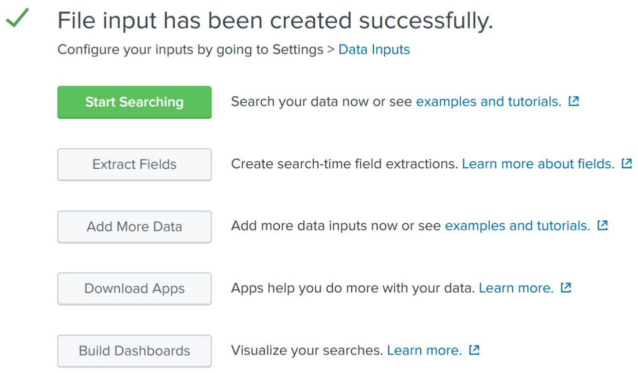


Source type: default ▾

linux_secure

linux_secure
Format for the /var/log/secure file containing all security related messages on a Linux machine

- Perform the final review and then start searching



✓ File input has been created successfully.

Configure your inputs by going to Settings > Data Inputs

Search your data now or see examples and tutorials.

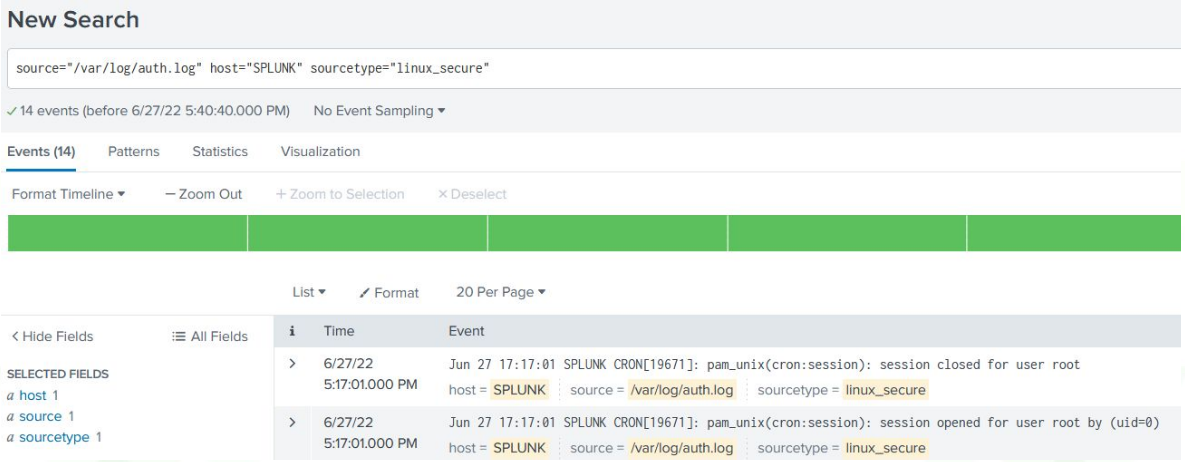
Create search-time field extractions. Learn more about fields.

Add more data inputs now or see examples and tutorials.

Apps help you do more with your data. Learn more.

Visualize your searches. Learn more.

- Monitor the events in real-time



New Search

```
source="/var/log/auth.log" host="SPLUNK" sourcetype="linux_secure"
```

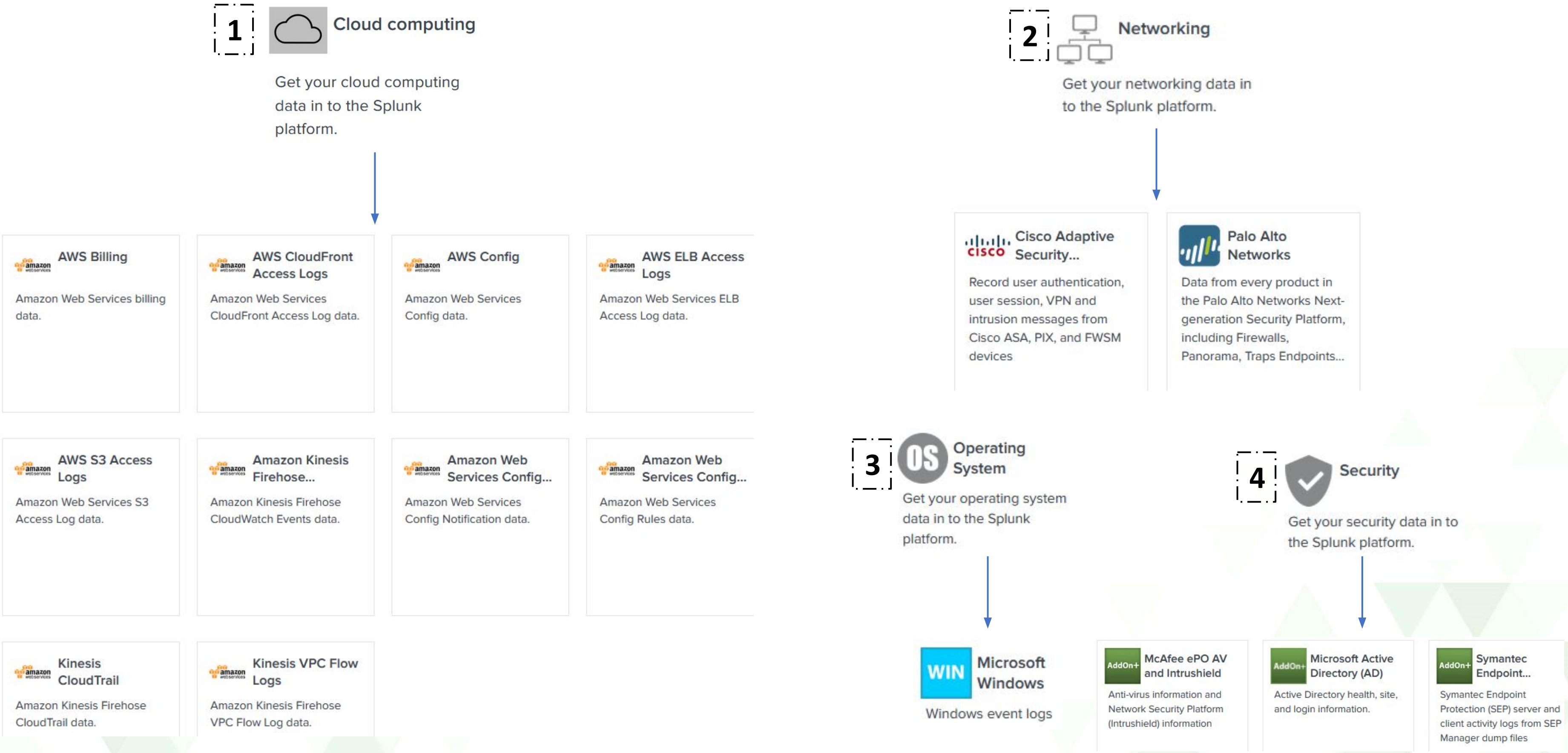
✓ 14 events (before 6/27/22 5:40:40.000 PM)

SELECTED FIELDS

a host	1
a source	1
a sourcetype	1

i	Time	Event
>	6/27/22 5:17:01.000 PM	Jun 27 17:17:01 SPLUNK CRON[19671]: pam_unix(cron:session): session closed for user root host = SPLUNK source = /var/log/auth.log sourcetype = linux_secure
>	6/27/22 5:17:01.000 PM	Jun 27 17:17:01 SPLUNK CRON[19671]: pam_unix(cron:session): session opened for user root by (uid=0) host = SPLUNK source = /var/log/auth.log sourcetype = linux_secure

- Log collection other sources



1 Cloud computing

Get your cloud computing data in to the Splunk platform.

AWS Billing

Amazon Web Services billing data.

AWS CloudFront Access Logs

Amazon Web Services CloudFront Access Log data.

AWS Config

Amazon Web Services Config data.

AWS ELB Access Logs

Amazon Web Services ELB Access Log data.

AWS S3 Access Logs

Amazon Web Services S3 Access Log data.

Amazon Kinesis Firehose...

Amazon Kinesis Firehose CloudWatch Events data.

Amazon Web Services Config...

Amazon Web Services Config Notification data.

Amazon Web Services Config...

Amazon Web Services Config Rules data.

Kinesis CloudTrail

Amazon Kinesis Firehose CloudTrail data.

Kinesis VPC Flow Logs

Amazon Kinesis Firehose VPC Flow Log data.

2 Networking

Get your networking data in to the Splunk platform.

Cisco Adaptive Security...

Record user authentication, user session, VPN and intrusion messages from Cisco ASA, PIX, and FWSM devices

Palo Alto Networks

Data from every product in the Palo Alto Networks Next-generation Security Platform, including Firewalls, Panorama, Traps Endpoints...

3 Operating System

Get your operating system data in to the Splunk platform.

Microsoft Windows

Windows event logs

4 Security

Get your security data in to the Splunk platform.

McAfee ePO AV and Intrushield

Anti-virus information and Network Security Platform (Intrushield) information

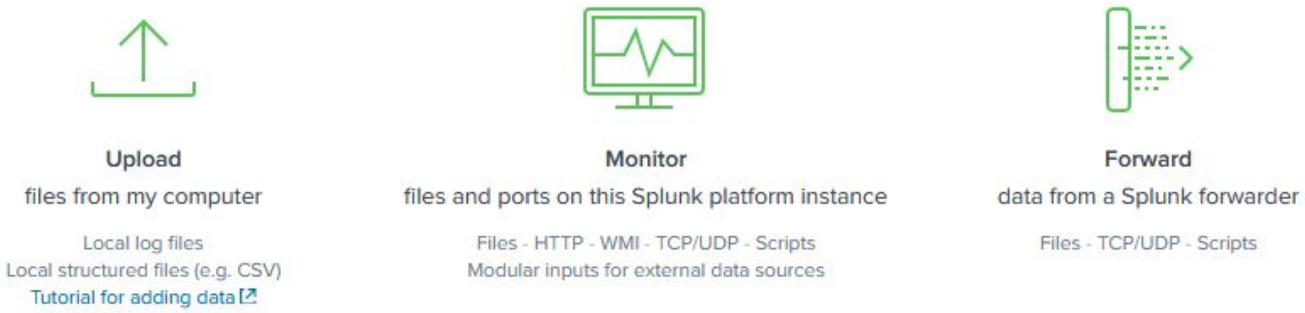
Microsoft Active Directory (AD)

Active Directory health, site, and login information.

Symantec Endpoint...

Symantec Endpoint Protection (SEP) server and client activity logs from SEP Manager dump files

5



Upload

files from my computer

Local log files
Local structured files (e.g. CSV)
Tutorial for adding data

Monitor

files and ports on this Splunk platform instance

Files - HTTP - WMI - TCP/UDP - Scripts
Modular inputs for external data sources

Forward

data from a Splunk forwarder

Files - TCP/UDP - Scripts

DEMO : Install Splunk in Linux Instance

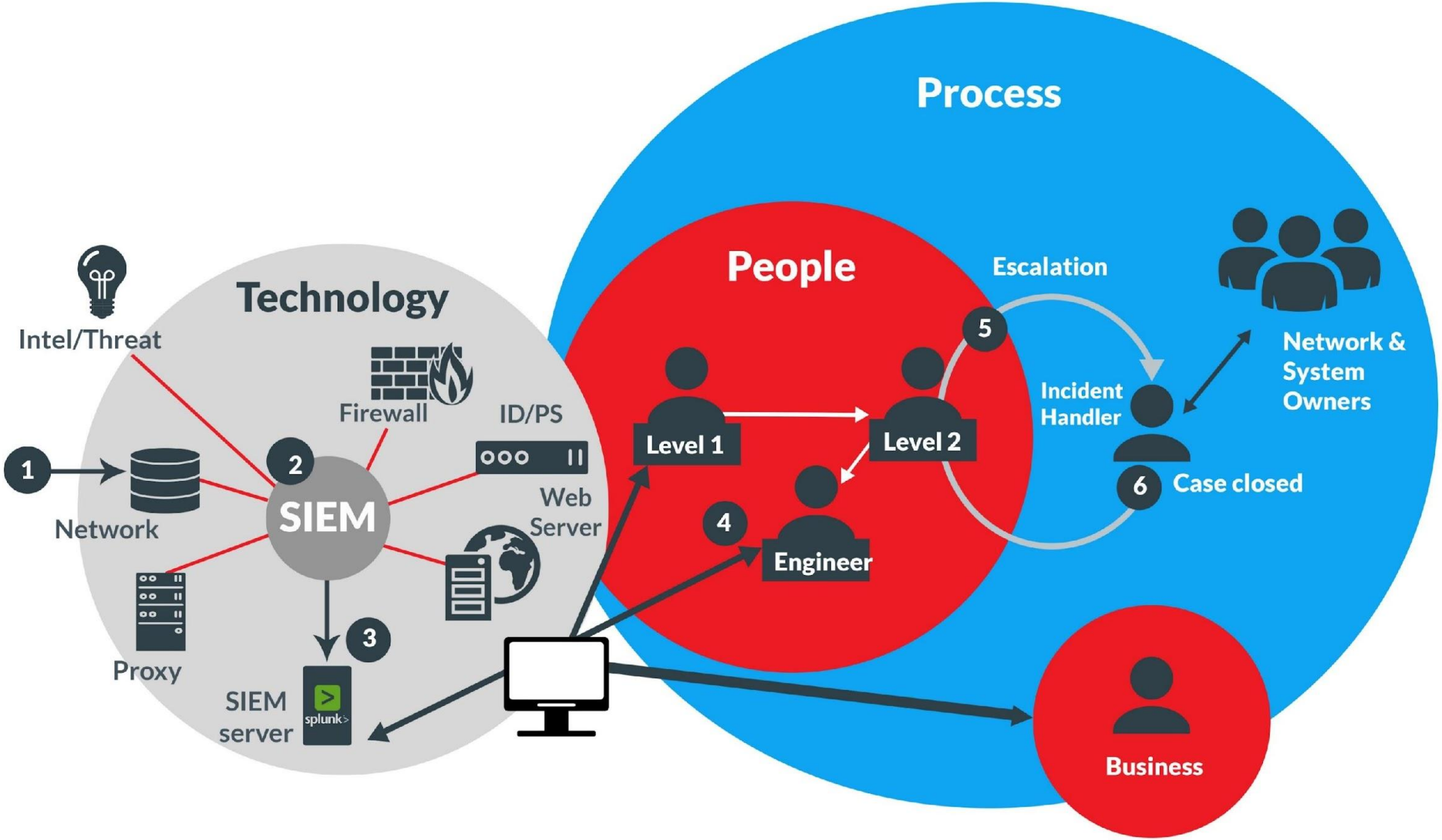
DEMO : Log forwarding to Splunk

1. Installing “sysmon” in Windows Machine
2. Collecting & Transferring logs via “Universal Forwarder (UF)”

DEMO : Log forwarding to Splunk

1. Installing “sysmon” in Windows Machine
2. Collecting & Transferring logs via “Universal Forwarder (UF)”

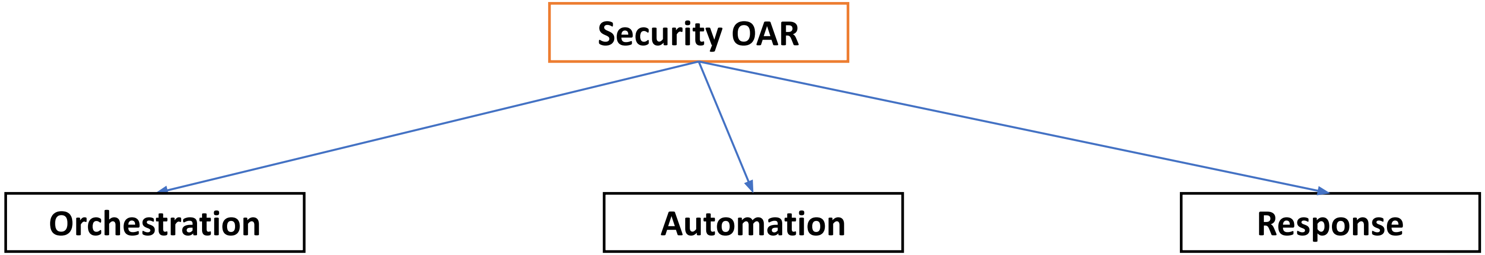
Concept of operations



@ CyberWarFare Labs

- **Security Orchestration, Automation and Response – Azure Sentinel**

  - It is a technology that allows organizations to collect data (alerts + events) & allows analysts to respond to threats in real-time using repetitive tasks



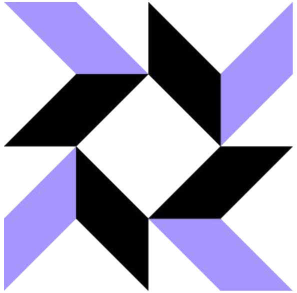
Threat & Vulnerability Management

Automate particular areas of security operations

Security Incident Response to strategically increase the effectiveness of Security Operations

- **OSQuery 101**

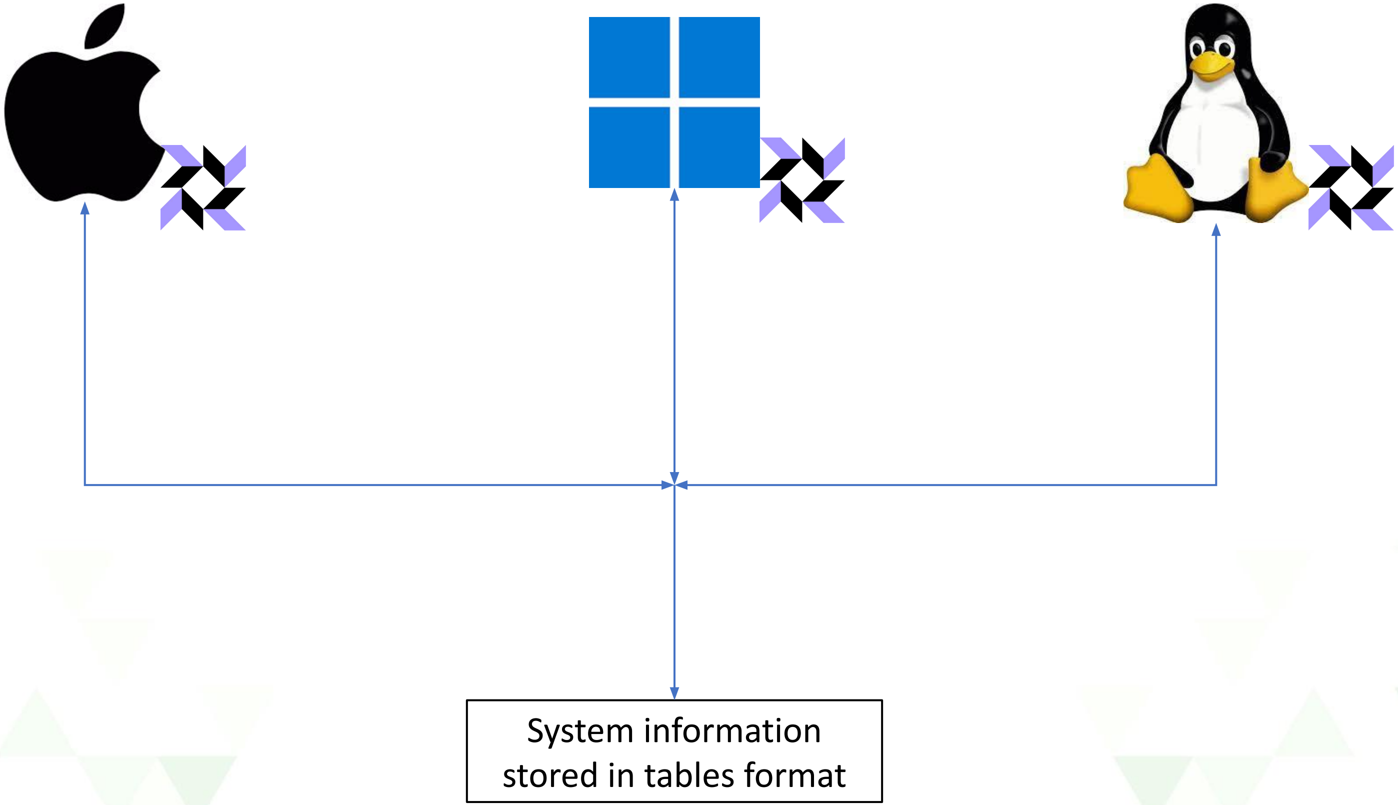
  - OSQuery framework originally developed by Meta, exposes an OS as a high-operational database.



  - Data like system network connection, running processes etc is stored in tables

  - We can extract the system data using SQL queries from the tables

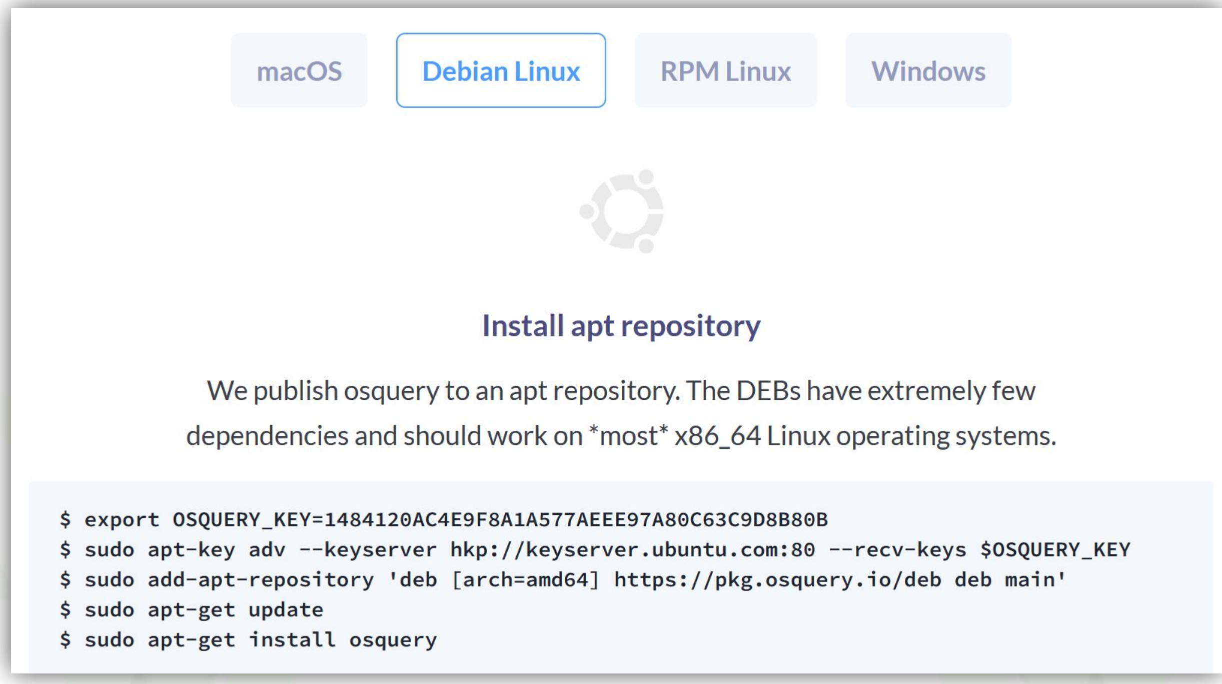
  - Extracted information can then be feed to SIEM servers etc for further processing



System information stored in tables format

- Install OSQuery (Linux)

Link : https://osquery.io/downloads/



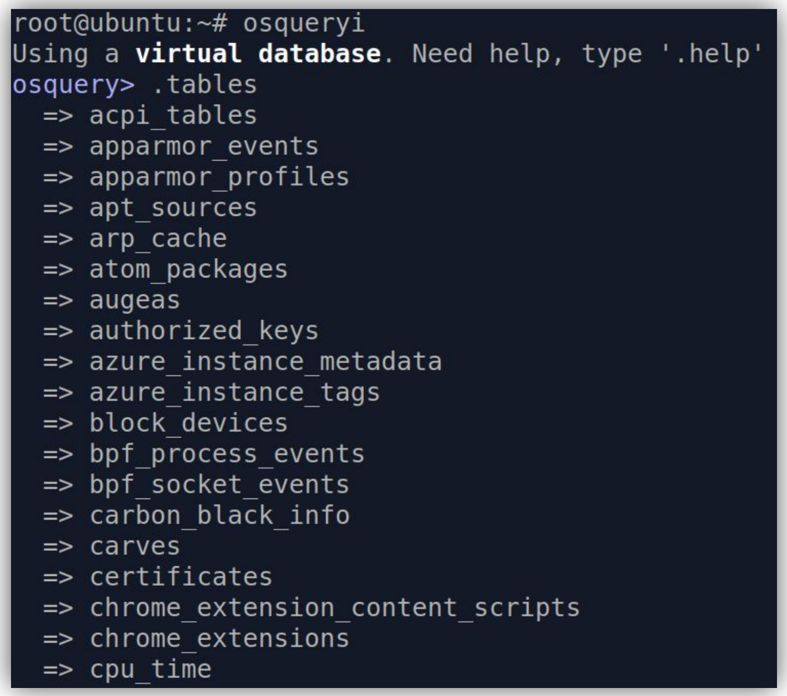
Install apt repository

We publish osquery to an apt repository. The DEBs have extremely few dependencies and should work on *most* x86_64 Linux operating systems.

```
$ export OSQUERY_KEY=1484120AC4E9F8A1A577AEEE97A80C63C9D8B80B
$ sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys $OSQUERY_KEY
$ sudo add-apt-repository 'deb [arch=amd64] https://pkg.osquery.io/deb deb main'
$ sudo apt-get update
$ sudo apt-get install osquery
```

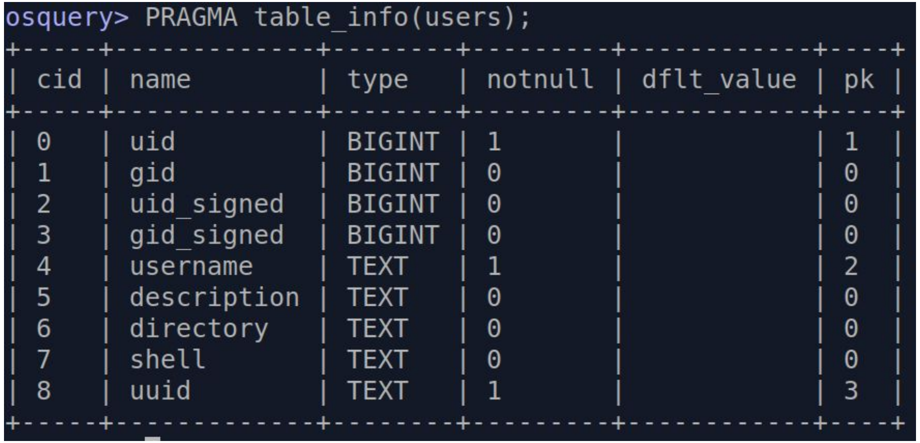
Exercise : Install OSQUERY in Linux Instance

- Run and check all the available tables:



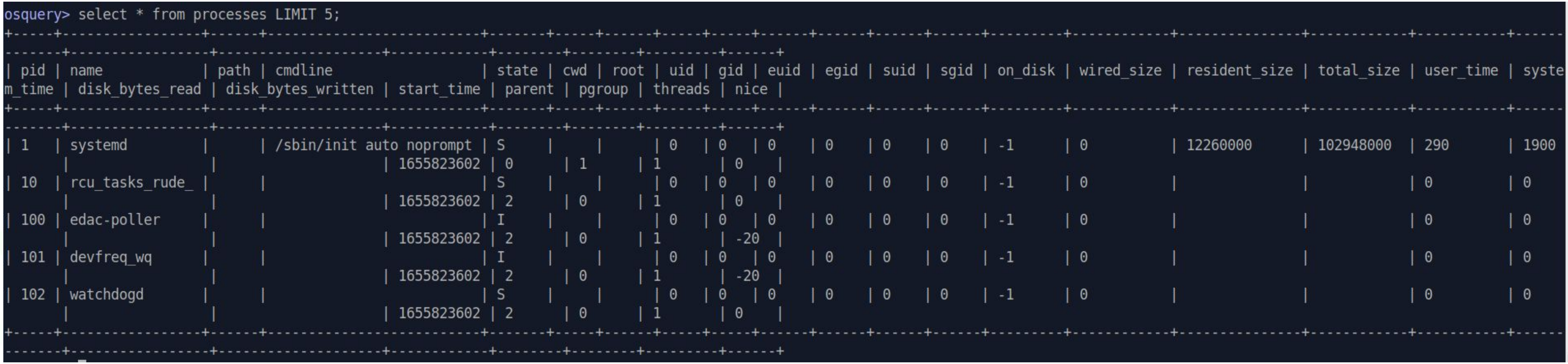
```
root@ubuntu:~# osqueryi
Using a virtual database. Need help, type '.help'
osquery> .tables
  => acpi_tables
  => apparmor_events
  => apparmor_profiles
  => apt_sources
  => arp_cache
  => atom_packages
  => augeas
  => authorized_keys
  => azure_instance_metadata
  => azure_instance_tags
  => block_devices
  => bpf_process_events
  => bpf_socket_events
  => carbon_black_info
  => carves
  => certificates
  => chrome_extension_content_scripts
  => chrome_extensions
  => cpu_time
```

- Check the structure of each table



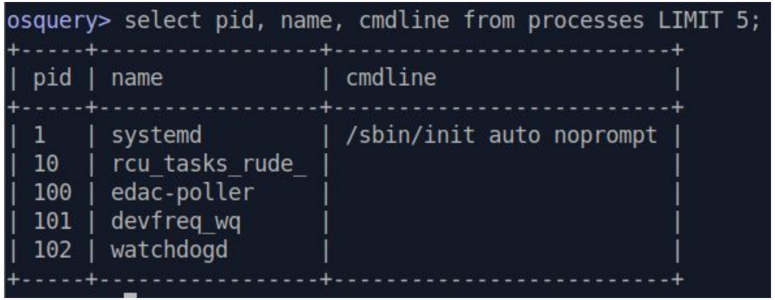
```
osquery> PRAGMA table_info(users);
+-----+-------------+--------+---------+------------+----+
| cid | name        | type   | notnull | dflt_value | pk |
+-----+-------------+--------+---------+------------+----+
| 0   | uid         | BIGINT | 1       |            | 1  |
| 1   | gid         | BIGINT | 0       |            | 0  |
| 2   | uid_signed  | BIGINT | 0       |            | 0  |
| 3   | gid_signed  | BIGINT | 0       |            | 0  |
| 4   | username    | TEXT   | 1       |            | 2  |
| 5   | description | TEXT   | 0       |            | 0  |
| 6   | directory   | TEXT   | 0       |            | 0  |
| 7   | shell       | TEXT   | 0       |            | 0  |
| 8   | uuid        | TEXT   | 1       |            | 3  |
+-----+-------------+--------+---------+------------+----+
```

- Query from a table and limit the results



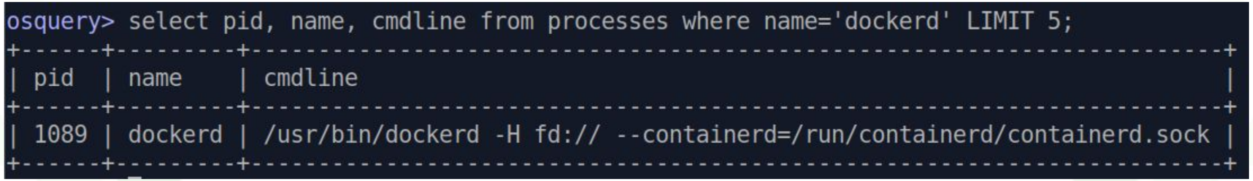
```
osquery> select * from processes LIMIT 5;
+-----+-----------------+------+--------------------------+-------+-----+------+-----+-----+------+------+------+------+---------+------------+---------------+------------+-----------+------
-------+-----------------+--------------------+------------+--------+--------+---------+------+
| pid | name            | path | cmdline                  | state | cwd | root | uid | gid | euid | egid | suid | sgid | on_disk | wired_size | resident_size | total_size | user_time | syste
m_time | disk_bytes_read | disk_bytes_written | start_time | parent | pgroup | threads | nice |
+-----+-----------------+------+--------------------------+-------+-----+------+-----+-----+------+------+------+------+---------+------------+---------------+------------+-----------+------
-------+-----------------+--------------------+------------+--------+--------+---------+------+
| 1   | systemd         |      | /sbin/init auto noprompt | S     |     |      | 0   | 0   | 0    | 0    | 0    | 0    | -1      | 0          | 12260000      | 102948000  | 290       | 1900
       |                 |                    | 1655823602 | 0      | 1      | 1       | 0    |
| 10  | rcu_tasks_rude_ |      |                          | S     |     |      | 0   | 0   | 0    | 0    | 0    | 0    | -1      | 0          |               |            | 0         | 0
       |                 |                    | 1655823602 | 2      | 0      | 1       | 0    |
| 100 | edac-poller     |      |                          | I     |     |      | 0   | 0   | 0    | 0    | 0    | 0    | -1      | 0          |               |            | 0         | 0
       |                 |                    | 1655823602 | 2      | 0      | 1       | -20  |
| 101 | devfreq_wq      |      |                          | I     |     |      | 0   | 0   | 0    | 0    | 0    | 0    | -1      | 0          |               |            | 0         | 0
       |                 |                    | 1655823602 | 2      | 0      | 1       | -20  |
| 102 | watchdogd       |      |                          | S     |     |      | 0   | 0   | 0    | 0    | 0    | 0    | -1      | 0          |               |            | 0         | 0
       |                 |                    | 1655823602 | 2      | 0      | 1       | 0    |
+-----+-----------------+------+--------------------------+-------+-----+------+-----+-----+------+------+------+------+---------+------------+---------------+------------+-----------+------
-------+-----------------+--------------------+------------+--------+--------+---------+------+
```

- Selecting 2 columns from a table



```
osquery> select pid, name, cmdline from processes LIMIT 5;
+-----+-----------------+--------------------------+
| pid | name            | cmdline                  |
+-----+-----------------+--------------------------+
| 1   | systemd         | /sbin/init auto noprompt |
| 10  | rcu_tasks_rude_ |                          |
| 100 | edac-poller     |                          |
| 101 | devfreq_wq      |                          |
| 102 | watchdogd       |                          |
+-----+-----------------+--------------------------+
```

- With Filtering



```
osquery> select pid, name, cmdline from processes where name='dockerd' LIMIT 5;
+------+---------+------------------------------------------------------------------------+
| pid  | name    | cmdline                                                                |
+------+---------+------------------------------------------------------------------------+
| 1089 | dockerd | /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock |
+------+---------+------------------------------------------------------------------------+
```

Exercise : Explore the Tables & Replicate the above exercises

Final Examination Instructions

- Once the self-paced materials are thoroughly completed, please reach out at **support@cyberwarfare.live** to schedule the examination
- The exam project would be of **20 Days,** starting from the day when the Support team shares the details with you as per your schedule
- The project solution report must be in **PDF** format

Final Examination Instructions

- Candidates can follow any **report template**, however the steps & documentation must be clear & thorough

- Candidates can submit the **PDF** report via email within the mentioned Duration (**20 Days**)

- Evaluators will provide the results within **3 working days**

CYBERWARFARE LABS
RESEARCH AND DEVELOPMENT CENTER
CWL
WARFARE IN CYBER SPACE

Thank you!

For any technical support, please mail at:
support@cyberwarfare.live